BAN CHẤP HÀNH TRUNG ƯƠNG
VĂN PHÒNG
*
Số 556-QĐ/VPTW

ĐẢNG CỘNG SẢN VIỆT NAM

Hà Nội, ngày 06 tháng 9 năm 2026

QUYẾT ĐỊNH
ban hành Quy định về xây dựng, triển khai, nghiệm thu, quản lý và vận hành hệ thống thông tin trong các cơ quan Đảng

---

- Căn cứ Nghị quyết số 57-NQ/TW, ngày 22/12/2024 của Bộ Chính trị về đột phá phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số quốc gia;

- Căn cứ Quyết định số 259-QĐ/TW, ngày 24/01/2025 của Bộ Chính trị khoá XIII về chức năng, nhiệm vụ, tổ chức bộ máy của Văn phòng Trung ương Đảng;

- Căn cứ Quy định số 384-QĐ/TW, ngày 19/11/2025 của Ban Bí thư về kết nối, chia sẻ dữ liệu giữa các cơ quan Đảng với các cơ quan, tổ chức khác trong hệ thống chính trị;

- Căn cứ Chỉ thị số 57-CT/TW, ngày 31/12/2025 của Ban Bí thư về tăng cường bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu trong hệ thống chính trị;

- Căn cứ Luật Chuyển đổi số 148/2025/QH15;

- Căn cứ Luật An ninh mạng số 116/2025/QH15;

- Căn cứ Luật Dữ liệu số 60/2024/QH15;

- Căn cứ Luật Giao dịch điện tử số 20/2023/QH15;

- Căn cứ Luật Bảo vệ bí mật nhà nước số 117/2025/QH15;

- Căn cứ Luật Trí tuệ nhân tạo số 134/2025/QH15;

- Căn cứ Luật Lưu trữ số 33/2024/QH15;

- Căn cứ Nghị định số 224/2026/NĐ-CP, ngày 24/6/2026 của Chính phủ quy định chi tiết một số điều và biện pháp thi hành Luật Chuyển đổi số;

- Căn cứ Nghị định số 331/2026/NĐ-CP, ngày 19/8/2026 của Chính phủ về bảo vệ an ninh mạng đối với hệ thống thông tin;

- Căn cứ Nghị định số 278/2025/NĐ-CP, ngày 22/10/2025 của Chính phủ quy định về kết nối, chia sẻ dữ liệu bắt buộc giữa các cơ quan thuộc hệ thống chính trị;

- Căn cứ Nghị định số 63/2026/NĐ-CP, ngày 28/02/2026 của Chính phủ quy định chi tiết một số điều và biện pháp thi hành Luật Bảo vệ bí mật nhà nước;

- Căn cứ Nghị định số 13/2023/NĐ-CP, ngày 17/4/2023 của Chính phủ về bảo vệ dữ liệu cá nhân;

- Căn cứ Nghị định số 68/2024/NĐ-CP, ngày 25/6/2024 của Chính phủ quy định về chữ ký số chuyên dùng công vụ;

- Căn cứ Quyết định số 1425/QĐ-TTg, ngày 29/7/2026 của Thủ tướng Chính phủ ban hành Khung kiến trúc tổng thể quốc gia số, phiên bản 1.0;

- Căn cứ Quyết định số 480-QĐ/TW, ngày 26/8/2026 của Ban Bí thư ban hành Khung Kiến trúc số trong các cơ quan Đảng, phiên bản 1.0;

- Căn cứ Thông tư số 39/2026/TT-BKHCN, ngày 01/7/2026 của Bộ trưởng Bộ Khoa học và Công nghệ quy định lập và quản lý chi phí trong hoạt động đầu tư, mua sắm, thuê dịch vụ cho chuyển đổi số sử dụng ngân sách nhà nước;

- Căn cứ Thông tư số 41/2026/TT-BKHCN, ngày 01/7/2026 của Bộ trưởng Bộ Khoa học và Công nghệ quy định chi tiết về phát triển thử nghiệm trong chuyển đổi số và quản lý chất lượng các hoạt động đầu tư, mua sắm, thuê dịch vụ cho chuyển đổi số sử dụng ngân sách nhà nước;

- Xét đề nghị của Cục Chuyển đổi số - Cơ yếu.

CHÁNH VĂN PHÒNG TRUNG ƯƠNG ĐẢNG
QUYẾT ĐỊNH

Điều 1. Ban hành kèm theo Quyết định này Quy định về xây dựng, triển khai, nghiệm thu, quản lý và vận hành hệ thống thông tin trong các cơ quan Đảng.

Điều 2. Các cơ quan, tổ chức đảng ở Trung ương và địa phương khi xây dựng, triển khai, nghiệm thu, quản lý và vận hành hệ thống thông tin thuộc phạm vi quản lý, sử dụng, kết nối, chia sẻ dữ liệu hoặc dùng chung trong các cơ quan Đảng có trách nhiệm thực hiện Quyết định này.

Các cơ quan, tổ chức khác khi kết nối, chia sẻ dữ liệu, khai thác, phối hợp vận hành hoặc tham gia bảo đảm an ninh mạng, an ninh dữ liệu, an toàn dữ liệu, sao lưu, phục hồi, khôi phục sau sự cố đối với hệ thống thông tin của các cơ quan Đảng thực hiện Quyết định này trong phạm vi trách nhiệm có liên quan.

Điều 3. Giao Cục Chuyển đổi số - Cơ yếu là đơn vị đầu mối tham mưu, hướng dẫn, theo dõi, kiểm tra, đôn đốc việc thực hiện Quyết định này; tổng hợp khó khăn, vướng mắc, báo cáo Chánh Văn phòng Trung ương Đảng xem xét, quyết định hoặc báo cáo cấp có thẩm quyền đối với nội dung vượt thẩm quyền.

Điều 4. Quyết định này có hiệu lực kể từ ngày ký.

Nơi nhận:
- Như Điều 2,
- Đồng chí Chánh Văn phòng Trung ương Đảng (để báo cáo);
- Cục Chuyển đổi số - Cơ yếu;
- Lưu Văn phòng Trung ương Đảng.

K/T CHÁNH VĂN PHÒNG
PHÓ CHÁNH VĂN PHÒNG

ĐẢNG CỘNG SẢN VIỆT NAM
VĂN PHÒNG
BAN CHẤP HÀNH TRUNG ƯƠNG

Võ Thành Hưng

QUY ĐỊNH
về xây dựng, triển khai, nghiệm thu, quản lý và vận hành hệ thống thông tin trong các cơ quan Đảng

(Kèm theo Quyết định số 556-QĐ/VPTW, ngày 06/9/2026 của Văn phòng Trung ương Đảng)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

1. Quy định này điều chỉnh toàn bộ quá trình xây dựng, triển khai, nghiệm thu, quản lý và vận hành hệ thống thông tin trong các cơ quan Đảng, từ khi phát sinh nhu cầu, xác định bài toán nghiệp vụ, xây dựng đầu bài, lập phương án, thiết kế, triển khai, kiểm thử, nghiệm thu, bàn giao đến quản lý, vận hành, bảo trì, thay đổi, đánh giá, dừng khai thác, thay thế, chuyển giao hoặc thanh lý.

2. Quy định này là căn cứ thống nhất để quản lý hệ thống thông tin theo yêu cầu nghiệp vụ, dữ liệu và kiến trúc; bảo đảm phù hợp với Khung kiến trúc tổng thể quốc gia số, Khung Kiến trúc số trong các cơ quan Đảng và các tài liệu Kiến trúc số có liên quan.

3. Quy định này không thay thế các quy định pháp luật về quy trình, thủ tục về đầu tư, mua sắm, thuê dịch vụ, đấu thầu, đặt hàng, quản lý hợp đồng, nghiệm thu khối lượng, thanh toán, quyết toán, quản lý tài sản hoặc trình tự, thủ tục chuyên ngành về bảo vệ an ninh mạng đối với hệ thống thông tin theo cấp độ. Các cơ quan, đơn vị, tổ chức, cá nhân có liên quan có trách nhiệm, ngoài việc thực hiện Quy định này, tuân thủ đầy đủ các quy định pháp luật hiện hành đối với các nội dung này khi xây dựng, triển khai, nghiệm thu, quản lý và vận hành hệ thống thông tin trong các cơ quan Đảng.

4. Các yêu cầu về hồ sơ, biểu mẫu và điểm kiểm soát tại Quy định này nhằm phục vụ quản trị vòng đời hệ thống thông tin, không làm phát sinh thủ tục trùng lặp với quy định chuyên ngành. Trường hợp pháp luật chuyên ngành, hồ sơ nhiệm vụ, dự án, mua sắm, thuê dịch vụ, hợp đồng hoặc quy định của cấp có thẩm quyền đã có tài liệu tương đương và bảo đảm đầy đủ nội dung cần kiểm soát theo Quy định này thì được sử dụng tài liệu đó.

5. Đối với hệ thống thông tin có tạo lập, xử lý, lưu trữ, truyền đưa, hiển thị, khai thác, tích hợp, chia sẻ hoặc sao lưu thông tin thuộc danh mục bí mật nhà nước, dữ liệu cá nhân, dữ liệu cá nhân nhạy cảm, dữ liệu nội bộ nhạy cảm,

dữ liệu hạn chế truy cập, ngoài việc thực hiện Quy định này còn phải tuân thủ quy định của Đảng, pháp luật của Nhà nước về bảo vệ bí mật nhà nước, cơ yếu, bảo vệ dữ liệu cá nhân, bảo vệ an ninh mạng đối với hệ thống thông tin theo cấp độ, quản lý rủi ro an ninh mạng, an ninh dữ liệu, an toàn dữ liệu, bảo mật thông tin, sao lưu, phục hồi, khôi phục sau sự cố và các quy định có liên quan.

Điều 2. Đối tượng áp dụng

1. Cơ quan chủ quản hệ thống thông tin; chủ đầu tư hoặc cơ quan, đơn vị được giao quản lý nhiệm vụ, dự án, hoạt động mua sắm, thuê dịch vụ, xây dựng, nâng cấp, mở rộng hệ thống thông tin.

2. Đơn vị chủ trì sử dụng, đơn vị đề xuất nhu cầu, đơn vị khai thác hệ thống thông tin trong thực tiễn nghiệp vụ.

3. Đơn vị chuyên trách về chuyển đổi số; đơn vị chuyên trách về an ninh mạng, an ninh dữ liệu hoặc đầu mối được giao nhiệm vụ bảo vệ an ninh mạng, an toàn dữ liệu; đơn vị cơ yếu; đơn vị quản lý hạ tầng kỹ thuật; đơn vị quản lý, vận hành hệ thống thông tin.

4. Chủ quản dữ liệu, đơn vị quản trị dữ liệu, đơn vị tạo lập, cập nhật, cung cấp, khai thác, chia sẻ dữ liệu.

5. Nhà thầu, đơn vị tư vấn, thiết kế, phát triển, kiểm thử, cung cấp phần mềm thương mại, cung cấp dịch vụ công nghệ số, bảo trì, hỗ trợ kỹ thuật; người sử dụng hệ thống thông tin; cơ quan, tổ chức khác trong hệ thống chính trị khi kết nối, chia sẻ dữ liệu, phối hợp vận hành hoặc tham gia bảo đảm an ninh mạng, an ninh dữ liệu, an toàn dữ liệu, sao lưu, phục hồi, khôi phục sau sự cố theo phạm vi trách nhiệm được giao.

Điều 3. Giải thích từ ngữ

1. Hệ thống thông tin là tập hợp hạ tầng kỹ thuật, phần mềm, cơ sở dữ liệu, các quy chế, quy định, quy trình quản lý, vận hành và nhân lực có liên quan, được thiết lập để tạo lập, thu thập, xử lý, lưu trữ, gửi nhận, khai thác, chia sẻ thông tin, dữ liệu phục vụ hoạt động của cơ quan, tổ chức, cá nhân.

2. Phần mềm là bộ mã lệnh (còn gọi là chương trình, ứng dụng, nền tảng) được thiết kế, phát triển, cấu hình để xử lý nghiệp vụ, dữ liệu, tương tác với người dùng, tích hợp hệ thống hoặc cung cấp dịch vụ số. Trong phạm vi Quy định này, phần mềm là một thành phần cấu thành nên hệ thống thông tin; không sử dụng thay thế cho khái niệm hệ thống thông tin. Trong đó:

- Phần mềm nội bộ là phần mềm được thiết kế, xây dựng, phát triển, nâng cấp, mở rộng theo yêu cầu riêng nhằm đáp ứng nhu cầu đặc thù của cơ quan, tổ chức, đơn vị, cá nhân.

- Phần mềm thương mại là phần mềm sẵn có, được cung cấp ngay khi có nhu cầu mà không phải thông qua đặt hàng thiết kế, xây dựng, phát triển, nâng cấp, mở rộng theo yêu cầu riêng.

3. Dịch vụ công nghệ số là việc cung cấp sản phẩm, nền tảng, phần mềm, hạ tầng, công cụ, dữ liệu hoặc năng lực công nghệ số dưới dạng dịch vụ để cơ quan, tổ chức, cá nhân khai thác, sử dụng theo thoả thuận, hợp đồng hoặc điều kiện dịch vụ được phê duyệt.

4. Cổng ứng dụng của các cơ quan Đảng là môi trường tập trung để công bố, tích hợp, truy cập hoặc khai thác các ứng dụng thành phần phục vụ hoạt động của các cơ quan Đảng theo mô hình được cấp có thẩm quyền phê duyệt. Ứng dụng thành phần trên Cổng là phần mềm, dịch vụ hoặc chức năng được đưa lên Cổng ứng dụng để người dùng truy cập, khai thác theo phân quyền.

5. Hệ thống thông tin có xử lý thông tin mật là hệ thống thông tin có tạo lập, xử lý, lưu trữ, gửi nhận, hiển thị, khai thác hoặc sao lưu thông tin thuộc danh mục bí mật nhà nước.

6. Chủ quản hệ thống thông tin là cơ quan, tổ chức, đơn vị, cá nhân có thẩm quyền quản lý trực tiếp hoặc được giao quản lý đối với hệ thống thông tin; trực tiếp chỉ đạo, chịu trách nhiệm tổ chức bảo vệ an ninh mạng đối với hệ thống thông tin thuộc phạm vi quản lý; chịu trách nhiệm về mục tiêu, phạm vi, dữ liệu, an ninh mạng, an ninh dữ liệu, an toàn dữ liệu, khả năng vận hành liên tục, hiệu quả khai thác và tổ chức vận hành hệ thống theo thẩm quyền.

7. Chủ đầu tư hoặc đơn vị được giao quản lý nhiệm vụ, dự án là cơ quan, đơn vị được cấp có thẩm quyền giao tổ chức thực hiện nhiệm vụ, dự án, hoạt động mua sắm, thuê dịch vụ, xây dựng, nâng cấp, mở rộng hệ thống thông tin theo quy định.

8. Đơn vị chủ trì sử dụng là đơn vị đề xuất nhu cầu, xác định bài toán nghiệp vụ, yêu cầu sử dụng, yêu cầu dữ liệu nghiệp vụ; tham gia kiểm thử, vận hành thử, nghiệm thu sử dụng và chịu trách nhiệm về tính đúng, đủ, phù hợp, hợp pháp của yêu cầu nghiệp vụ, dữ liệu nghiệp vụ và nội dung xác nhận trong quá trình kiểm thử, vận hành thử, nghiệm thu.

9. Chủ quản dữ liệu là cơ quan, tổ chức, đơn vị có thẩm quyền quản lý, quyết định mục đích, phạm vi, phương thức tạo lập, cập nhật, khai thác, chia sẻ, lưu trữ, chỉnh sửa, chuyển đổi, thu hồi, tiêu huỷ hoặc lưu trữ lâu dài đối với dữ liệu thuộc phạm vi được giao.

10. Đơn vị quản trị dữ liệu là đơn vị được giao tổ chức quản lý kỹ thuật đối với dữ liệu, gồm cấu trúc dữ liệu, chuẩn dữ liệu, mã định danh, phân quyền, nhật ký, truy vết, sao lưu, đối soát, tích hợp và điều kiện kỹ thuật phục vụ quản lý dữ liệu.

11. Bài toán nghiệp vụ là tài liệu mô tả nhu cầu, hiện trạng, vấn đề cần giải quyết, mục tiêu nghiệp vụ, quy trình nghiệp vụ, yêu cầu chức năng, yêu cầu dữ liệu, yêu cầu phi chức năng và kết quả kỳ vọng do đơn vị chủ trì sử dụng đề xuất.

12. Đầu bài là tài liệu mô tả yêu cầu nghiệp vụ, dữ liệu, kỹ thuật, tích hợp, an ninh mạng, an ninh dữ liệu, an toàn dữ liệu, sao lưu, phục hồi, vận hành liên tục, nghiệm thu và các yêu cầu liên quan của hệ thống thông tin, làm căn cứ lập phương án xây dựng, triển khai, thuê, mua hệ thống thông tin.

13. Phương án xây dựng, triển khai là tài liệu xác định mục tiêu, phạm vi, kiến trúc, công nghệ, mô hình triển khai, yêu cầu dữ liệu, tích hợp, an ninh mạng, an ninh dữ liệu, an toàn dữ liệu, sao lưu, phục hồi, vận hành liên tục, kiểm thử, vận hành thử, nghiệm thu, bàn giao, vận hành, bảo trì, tiến độ và phân công trách nhiệm.

14. Hồ sơ hoàn thành là tập hợp hồ sơ, tài liệu hình thành trong quá trình xây dựng, triển khai, kiểm thử, vận hành thử, nghiệm thu, bàn giao hệ thống thông tin, được lưu trữ để phục vụ vận hành, bảo trì, kiểm tra, đánh giá, xử lý sự cố, nâng cấp, thay thế hoặc dừng khai thác.

15. Quản lý thay đổi là việc tiếp nhận, đánh giá, phê duyệt, kiểm thử, triển khai, giám sát và lưu hồ sơ đối với thay đổi về nghiệp vụ, chức năng, dữ liệu, cấu hình, tích hợp, hạ tầng, phân quyền, an ninh mạng, an ninh dữ liệu, an toàn dữ liệu, sao lưu, phục hồi, vận hành liên tục và chính sách vận hành sau khi hệ thống đã triển khai.

16. Cấp độ của hệ thống thông tin là cấp độ an ninh mạng của hệ thống thông tin được xác định theo quy định của pháp luật về an ninh mạng, căn cứ loại thông tin, loại hệ thống thông tin, mức độ ảnh hưởng, thiệt hại có thể xảy ra khi hệ thống bị xâm phạm, mất kiểm soát, gián đoạn, bị phá hoại, lộ lọt, mất, sai lệch hoặc không sẵn sàng; trường hợp hệ thống đồng thời thuộc nhiều tiêu chí cấp độ khác nhau thì áp dụng cấp độ cao hơn.

17. Hồ sơ xác định cấp độ là tập hợp hồ sơ, tài liệu phục vụ việc đề xuất, thẩm định, phê duyệt hoặc điều chỉnh cấp độ của hệ thống thông tin và phương án bảo vệ an ninh mạng theo cấp độ, gồm hồ sơ đề xuất cấp độ, hồ sơ phê duyệt cấp độ và các tài liệu liên quan theo quy định của pháp luật về an ninh mạng.

18. Đơn vị chuyên trách về an ninh mạng là đơn vị có chức năng, nhiệm vụ bảo đảm an ninh mạng của chủ quản hệ thống thông tin. Trường hợp cơ quan, đơn vị chưa có đơn vị chuyên trách riêng, thì người đứng đầu cơ quan chủ quản hệ thống thông tin chỉ định bộ phận, cá nhân phụ trách hoặc giao đơn vị chuyên trách chuyển đổi số thực hiện nhiệm vụ chuyên trách về an ninh mạng theo quy định.

19. Đơn vị vận hành hệ thống thông tin là đơn vị được chủ quản hệ thống thông tin giao nhiệm vụ vận hành hệ thống. Trường hợp hệ thống gồm nhiều thành phần hoặc do nhà thầu, đơn vị cung cấp dịch vụ vận hành theo hợp đồng, thì hồ sơ phải xác định rõ trách nhiệm vận hành, quyền quản trị, phạm vi hỗ trợ, thời hạn duy trì và trách nhiệm bàn giao, chuyển giao khi kết thúc dịch vụ.

20. Kiến trúc số giải pháp là mô tả kiến trúc của một nhiệm vụ, dự án, hệ thống thông tin hoặc thay đổi lớn, làm rõ nghiệp vụ, dữ liệu, ứng dụng, nền tảng, hạ tầng, tích hợp, an toàn, an ninh mạng, bảo vệ dữ liệu, vận hành và quan hệ với các tài liệu Kiến trúc số có liên quan.

21. Nguồn dữ liệu có thẩm quyền là hệ thống hoặc chủ thể được giao quyền xác lập, cập nhật và chịu trách nhiệm về giá trị gốc của dữ liệu trong một ngữ cảnh nghiệp vụ xác định.

22. Ngoại lệ kiến trúc là nội dung chưa đáp ứng yêu cầu kiến trúc nhưng được cấp có thẩm quyền xem xét chấp thuận có thời hạn, có căn cứ, đánh giá rủi ro, biện pháp kiểm soát, chủ thể chịu trách nhiệm và lộ trình khắc phục, hội tụ hoặc kết thúc.

Điều 4. Nguyên tắc thực hiện

1. Việc triển khai, vận hành hệ thống thông tin phải tuân thủ quy định của Đảng, pháp luật của Nhà nước và quy định có liên quan; bảo đảm phù hợp với quy mô, mức độ quan trọng, cấp độ, tính chất dữ liệu, phạm vi sử dụng, kết nối, chia sẻ dữ liệu và mức độ rủi ro của hệ thống.

2. Hệ thống thông tin phải phù hợp với Khung Kiến trúc số trong các cơ quan Đảng và các tài liệu Kiến trúc số có liên quan; ưu tiên sử dụng, kế thừa, tái sử dụng nền tảng, hệ thống, dữ liệu và thành phần dùng chung; không đầu tư, thuê dịch vụ hoặc phát triển trùng lặp, phân tán.

3. An ninh mạng, an ninh dữ liệu, an toàn dữ liệu, bảo vệ bí mật nhà nước, bảo vệ dữ liệu cá nhân và quản lý rủi ro phải được xác định, kiểm soát ngay từ khi đề xuất nhu cầu và duy trì trong suốt vòng đời hệ thống thông tin, phù hợp với cấp độ, tính chất dữ liệu và mức độ rủi ro.

4. Yêu cầu nghiệp vụ phải được xác định trước yêu cầu kỹ thuật. Quy trình nghiệp vụ phải được rà soát, chuẩn hoá, đơn giản hoá trước khi số hoá; xác định rõ trách nhiệm, dữ liệu, người dùng, yêu cầu kết nối, tích hợp và các điều kiện bảo đảm an ninh, bảo mật.

5. Hệ thống thông tin phải được thiết kế, quản lý theo hướng lấy dữ liệu làm nền tảng; dữ liệu được tạo lập, cập nhật, quản lý tại nguồn có thẩm quyền, bảo đảm chất lượng và khả năng kết nối, chia sẻ, khai thác, tái sử dụng theo đúng thẩm quyền, mục đích và phạm vi được phép.

6. Việc ứng dụng trí tuệ nhân tạo phải phục vụ yêu cầu nghiệp vụ, bảo đảm quản trị, bảo vệ dữ liệu, an ninh, bảo mật và có sự giám sát của con người. Không sử dụng nền tảng trí tuệ nhân tạo công cộng để xử lý thông tin mật, dữ liệu cá nhân nhạy cảm, dữ liệu nội bộ nhạy cảm hoặc dữ liệu hạn chế truy cập khi chưa được cấp có thẩm quyền cho phép.

Điều 5. Phân loại hệ thống thông tin để áp dụng Quy định

1. Hệ thống thông tin được phân loại để xác định phạm vi hồ sơ, mức độ kiểm soát, yêu cầu thẩm định, kiểm thử, nghiệm thu, bàn giao, vận hành, giám sát và trách nhiệm của các chủ thể tham gia.

2. Việc phân loại căn cứ các tiêu chí: tính chất thông tin xử lý; tính chất nhiệm vụ; mức độ quan trọng; cấp độ của hệ thống thông tin; phạm vi phục vụ; mô hình quản trị.

3. Theo tính chất thông tin xử lý, hệ thống được phân loại thành: hệ thống có xử lý thông tin thuộc danh mục bí mật nhà nước; hệ thống không xử lý thông tin mật nhưng có xử lý dữ liệu cá nhân, dữ liệu cá nhân nhạy cảm, dữ liệu nội bộ nhạy cảm hoặc dữ liệu hạn chế truy cập; và hệ thống không thuộc các trường hợp nêu trên.

4. Theo tính chất nhiệm vụ, hệ thống được phân loại thành xây dựng mới; nâng cấp, mở rộng; mua sắm, cấu hình phần mềm thương mại; thuê dịch vụ công nghệ số; tiếp nhận chuyển giao, tài trợ, sử dụng thử, sử dụng nền tảng dùng chung; bảo trì, thay đổi, thay thế, dừng khai thác hệ thống hiện có. Các nội dung phát triển thử nghiệm, thử nghiệm có kiểm soát trong chuyển đổi số thực

hiện theo trình tự, thủ tục riêng quy định tại Điều 12 của Quy định này và quy định của pháp luật có liên quan.

5. Theo mức độ quan trọng, hệ thống được phân loại thành hệ thống thông thường, hệ thống quan trọng và hệ thống trọng yếu phục vụ lãnh đạo, chỉ đạo, điều hành hoặc có tác động lớn đến hoạt động của cơ quan Đảng nếu bị gián đoạn, mất dữ liệu, lộ lọt dữ liệu, sai lệch dữ liệu hoặc bị tấn công.

6. Căn cứ kết quả phân loại, hệ thống thông tin được xác định theo một trong ba nhóm áp dụng:

a) Nhóm áp dụng đầy đủ đối với hệ thống trọng yếu, hệ thống quan trọng, hệ thống dùng chung, hệ thống có xử lý thông tin mật, dữ liệu cá nhân, dữ liệu hạn chế truy cập, hệ thống có kết nối, chia sẻ dữ liệu rộng, hệ thống từ cấp độ 3 trở lên hoặc có yêu cầu vận hành liên tục;

b) Nhóm áp dụng rút gọn đối với hệ thống nội bộ quy mô nhỏ, cấp độ 1, cấp độ 2, ít người dùng, ít kết nối, không xử lý thông tin mật, không xử lý dữ liệu cá nhân, dữ liệu cá nhân nhạy cảm, dữ liệu nội bộ nhạy cảm, dữ liệu hạn chế truy cập và không tác động lớn đến hoạt động nghiệp vụ nếu gián đoạn;

c) Nhóm áp dụng đặc thù đối với phần mềm thương mại, dịch vụ công nghệ số, nền tảng dùng chung, dịch vụ điện toán đám mây, hệ thống thuê dịch vụ, hệ thống tiếp nhận chuyển giao, tài trợ, sử dụng thử hoặc phối hợp khai thác.

7. Hồ sơ, kiểm thử, nghiệm thu, bàn giao, vận hành và giám sát đối với từng nhóm áp dụng được xác định theo phụ lục hoặc hướng dẫn kèm theo; không áp dụng cùng một mức hồ sơ, kiểm soát và thủ tục kỹ thuật đối với mọi loại hệ thống. Việc áp dụng rút gọn hoặc đặc thù phải được nêu rõ trong hồ sơ, được xác nhận theo thẩm quyền và không làm giảm yêu cầu về bảo vệ bí mật nhà nước, bảo vệ dữ liệu cá nhân, bảo vệ dữ liệu, an ninh mạng và trách nhiệm vận hành.

Trường hợp một hệ thống đồng thời có dấu hiệu thuộc nhiều nhóm áp dụng, thực hiện yêu cầu kiểm soát cao hơn đối với từng nội dung có liên quan. Việc xác định là nhóm áp dụng đặc thù chỉ để lựa chọn hồ sơ, cách thức kiểm soát phù hợp với hình thức triển khai, không làm giảm các yêu cầu bắt buộc về bảo vệ bí mật nhà nước, bảo vệ dữ liệu cá nhân, an ninh mạng, phân quyền, nhật ký, sao lưu, phục hồi, xử lý sự cố và trách nhiệm vận hành.

8. Việc xác định hệ thống thông tin để phân loại, xác định cấp độ phải căn cứ chức năng nghiệp vụ, dữ liệu xử lý, đối tượng sử dụng, đối tượng vận hành,

đối tượng phục vụ, dịch vụ cung cấp và kết quả đầu ra; không chỉ căn cứ địa giới hành chính, mô hình triển khai, hạ tầng, thiết bị hoặc phạm vi đầu tư.

9. Không phân tách hệ thống thông tin thành nhiều hệ thống nhằm hạ thấp cấp độ. Trường hợp các hệ thống thành phần có phụ thuộc chặt chẽ, chia sẻ dữ liệu, cùng quy trình nghiệp vụ hoặc có khả năng gây tác động dây chuyền khi xảy ra sự cố thì phải xem xét trong một chỉnh thể khi phân loại, xác định cấp độ và phương án bảo vệ.

10. Trường hợp hệ thống xử lý nhiều loại thông tin, dữ liệu hoặc đáp ứng đồng thời nhiều tiêu chí cấp độ khác nhau thì xác định theo cấp độ cao nhất; trường hợp hệ thống chỉ kết nối, chia sẻ dữ liệu với hệ thống khác nhưng không phụ thuộc chức năng, vận hành thì có thể xác định cấp độ riêng theo phạm vi, rủi ro và thẩm quyền quản lý.

Chương II
TRÁCH NHIỆM CỦA CÁC CHỦ THỂ THAM GIA

Điều 6. Trách nhiệm của cơ quan chủ quản hệ thống thông tin và chủ đầu tư

1. Cơ quan chủ quản hệ thống thông tin chịu trách nhiệm chỉ đạo, quyết định hoặc trình cấp có thẩm quyền quyết định chủ trương xây dựng, nâng cấp, mở rộng, mua sắm, thuê dịch vụ, tiếp nhận chuyển giao, đưa vào vận hành, thay thế hoặc dừng khai thác hệ thống thông tin.

2. Cơ quan chủ quản hệ thống thông tin chịu trách nhiệm xác định mục tiêu, phạm vi, đối tượng sử dụng, mô hình quản trị, chủ quản dữ liệu, đơn vị vận hành, nguồn lực, yêu cầu bảo vệ an ninh mạng, bảo vệ bí mật nhà nước, bảo vệ dữ liệu cá nhân và hiệu quả khai thác hệ thống; bố trí hoặc chỉ định đơn vị, bộ phận, cá nhân chuyên trách về an ninh mạng theo quy định; người đứng đầu cơ quan chủ quản chịu trách nhiệm chỉ đạo tổ chức quản lý các nội dung này theo thẩm quyền.

3. Chủ đầu tư hoặc đơn vị được giao quản lý nhiệm vụ, dự án chịu trách nhiệm tổ chức tiếp nhận yêu cầu, khảo sát, xây dựng đầu bài, lập phương án, tổ chức thẩm định, trình phê duyệt hoặc phê duyệt theo thẩm quyền; tổ chức triển khai, kiểm thử, vận hành thử, nghiệm thu, bàn giao và lập hồ sơ hoàn thành.

4. Chủ đầu tư hoặc đơn vị được giao quản lý nhiệm vụ, dự án chịu trách nhiệm quản lý tiến độ, chất lượng, chi phí theo phạm vi được giao; quản lý hợp

đồng, nhà thầu, sản phẩm, hồ sơ, tài liệu, mã nguồn, dữ liệu, tài khoản, cấu hình, quyền quản trị, bảo mật thông tin và các tài sản kỹ thuật khác phát sinh trong quá trình thực hiện.

5. Đối với nhiệm vụ, dự án, hoạt động mua sắm, thuê dịch vụ thuộc phạm vi điều chỉnh của pháp luật chuyên ngành, chủ đầu tư hoặc đơn vị được giao quản lý nhiệm vụ, dự án thực hiện theo quy định chuyên ngành; đồng thời phải bảo đảm các yêu cầu về đầu bài, kiến trúc, dữ liệu, kiểm thử, nghiệm thu sử dụng, bàn giao, vận hành và hồ sơ hoàn thành theo Quy định này.

Điều 7. Trách nhiệm của đơn vị chủ trì sử dụng

1. Đơn vị chủ trì sử dụng chịu trách nhiệm đề xuất nhu cầu, xác định bài toán nghiệp vụ, mục tiêu, phạm vi sử dụng, đối tượng sử dụng, kết quả đầu ra, yêu cầu dữ liệu nghiệp vụ và tiêu chí nghiệm thu sử dụng đối với hệ thống thông tin.

2. Đơn vị chủ trì sử dụng chịu trách nhiệm rà soát, mô tả, chuẩn hoá quy trình nghiệp vụ trước khi số hoá; xác định rõ quy trình hiện tại, vấn đề cần giải quyết, quy trình sau số hoá, chức năng cần thiết, dữ liệu đầu vào, dữ liệu đầu ra, biểu mẫu, báo cáo, thống kê, tra cứu, phê duyệt và phân quyền sử dụng.

3. Đơn vị chủ trì sử dụng phối hợp trong quá trình khảo sát, xây dựng đầu bài, lập phương án, kiểm thử, vận hành thử, nghiệm thu và bàn giao; chịu trách nhiệm về tính đúng, đủ, phù hợp, hợp pháp của yêu cầu nghiệp vụ, yêu cầu dữ liệu nghiệp vụ, tiêu chí nghiệm thu sử dụng và nội dung xác nhận trong các giai đoạn này.

4. Khi nghiệp vụ thay đổi do sửa đổi quy định, thay đổi cơ cấu tổ chức, quy trình công tác hoặc yêu cầu quản lý, đơn vị chủ trì sử dụng phải kịp thời thông báo, đề xuất xử lý để đánh giá tác động và điều chỉnh hệ thống thông tin theo quy định.

Điều 8. Trách nhiệm của đơn vị chuyên trách chuyển đổi số, an ninh mạng, cơ yếu

1. Đơn vị chuyên trách chuyển đổi số tham gia ý kiến, thẩm định hoặc hướng dẫn thẩm định về sự phù hợp của đầu bài, phương án xây dựng, triển khai, Kiến trúc số giải pháp và thay đổi lớn của hệ thống với Khung Kiến trúc số trong các cơ quan Đảng, Kiến trúc số cấp cơ quan, Kiến trúc số chuyên ngành, Kiến trúc số trong các cơ quan Đảng tỉnh, thành phố có liên quan; kiến trúc dữ liệu, tiêu chuẩn kỹ thuật, kết nối, chia sẻ dữ liệu, khả năng dùng chung, tái sử dụng, mở rộng, vận hành và tránh đầu tư trùng lặp.

2. Đơn vị chuyên trách về an ninh mạng hoặc đầu mối được giao nhiệm vụ bảo vệ an ninh mạng tham gia ý kiến, thẩm định hoặc hướng dẫn thẩm định về cấp độ của hệ thống thông tin, hồ sơ xác định cấp độ, phương án bảo vệ an ninh mạng theo cấp độ, xác thực, phân quyền, nhật ký, giám sát, sao lưu, phục hồi, xử lý sự cố, quản lý rủi ro an ninh mạng; kiểm tra, đánh giá, kiểm thử an ninh mạng trước nghiệm thu, trước vận hành chính thức, định kỳ hằng năm hoặc khi có thay đổi lớn trong quá trình vận hành.

3. Đơn vị cơ yếu chủ trì hoặc phối hợp thẩm định, hướng dẫn, kiểm tra các nội dung về cơ yếu, mật mã, chứng thư số, chữ ký số, quản lý khoá, truyền nhận thông tin mật, môi trường xử lý thông tin mật và yêu cầu bảo vệ bí mật nhà nước thuộc phạm vi chức năng, nhiệm vụ được giao.

4. Đối với hệ thống trọng yếu, hệ thống có xử lý thông tin mật, hệ thống dùng chung quy mô lớn hoặc hệ thống kết nối, chia sẻ dữ liệu rộng, các đơn vị chuyên trách phối hợp xây dựng phương án giám sát tập trung, cảnh báo, tiếp nhận, xử lý sự cố và báo cáo theo quy định.

Điều 9. Trách nhiệm của đơn vị vận hành, chủ quản dữ liệu và đơn vị quản trị dữ liệu

1. Đơn vị vận hành chịu trách nhiệm tiếp nhận, quản lý, vận hành hệ thống thông tin sau khi được bàn giao; thực hiện biện pháp bảo vệ an ninh mạng theo hồ sơ xác định cấp độ và phương án đã được phê duyệt; thực hiện giám sát hoạt động, quản lý tài khoản, phân quyền, cấu hình, dung lượng, hiệu năng, nhật ký, sao lưu, phục hồi, cập nhật, vá lỗi, xử lý yêu cầu hỗ trợ, xử lý sự cố và phối hợp đánh giá rủi ro an ninh mạng.

2. Đơn vị vận hành duy trì tài liệu vận hành, nhật ký vận hành, nhật ký truy cập, nhật ký thay đổi, nhật ký sự cố; báo cáo định kỳ hằng năm hoặc đột xuất về tình trạng vận hành, chất lượng dịch vụ, sự cố, rủi ro, kết quả thực hiện biện pháp bảo vệ an ninh mạng, yêu cầu nâng cấp, tối ưu, thay thế hoặc dừng khai thác.

3. Đơn vị vận hành không được tự ý thay đổi mã nguồn, cấu hình, cơ sở dữ liệu, phân quyền, chính sách an ninh mạng, luồng tích hợp, hạ tầng vận hành hoặc phương án sao lưu, phục hồi nếu chưa được phê duyệt theo quy trình quản lý thay đổi.

4. Chủ quản dữ liệu chịu trách nhiệm xác định, quản lý danh mục dữ liệu, mục đích xử lý, phạm vi xử lý, chủ thể tạo lập, chủ thể cập nhật, chủ thể khai thác, quy tắc kiểm tra, đối soát, chất lượng dữ liệu, chuẩn dữ liệu, mã định danh, thời hạn lưu trữ, quyền truy cập và trách nhiệm chia sẻ dữ liệu.

5. Chủ quản dữ liệu chịu trách nhiệm về tính đầy đủ, chính xác, cập nhật, hợp pháp, phù hợp mục đích của dữ liệu thuộc phạm vi quản lý; kịp thời xử lý hoặc đề xuất xử lý dữ liệu sai lệch, thiếu, trùng lặp, không còn giá trị sử dụng, không đúng thẩm quyền hoặc không bảo đảm chất lượng.

6. Đơn vị quản trị dữ liệu chịu trách nhiệm về công cụ, cấu trúc dữ liệu, lược đồ dữ liệu, chuẩn dữ liệu, tích hợp dữ liệu, phân quyền dữ liệu, nhật ký dữ liệu, sao lưu dữ liệu, truy vết dữ liệu và điều kiện kỹ thuật phục vụ quản lý dữ liệu.

7. Chủ quản dữ liệu và đơn vị quản trị dữ liệu quản lý vòng đời dữ liệu song song với vòng đời hệ thống thông tin, gồm tạo lập, chuẩn hoá, phê duyệt, cập nhật, khai thác, chia sẻ, lưu trữ, chỉnh sửa, thu hồi, chuyển đổi, lưu trữ lâu dài hoặc tiêu huỷ dữ liệu theo quy định.

Điều 10. Trách nhiệm của nhà thầu, đơn vị cung cấp dịch vụ và người sử dụng

1. Nhà thầu, đơn vị tư vấn, đơn vị phát triển, kiểm thử, cung cấp phần mềm thương mại, cung cấp dịch vụ công nghệ số có trách nhiệm thực hiện đúng hợp đồng, hồ sơ yêu cầu, đầu bài, phương án xây dựng, thiết kế, yêu cầu nghiệp vụ, dữ liệu, kỹ thuật, an ninh mạng, bảo mật thông tin và tích hợp đã được phê duyệt.

2. Nhà thầu, đơn vị cung cấp dịch vụ có trách nhiệm bảo mật thông tin, dữ liệu, tài khoản, mã nguồn, cấu hình, sơ đồ hệ thống, tài liệu kỹ thuật, lỗ hổng, nhật ký và thông tin khác tiếp cận được trong quá trình thực hiện; không sử dụng, sao chép, chuyển giao, tiết lộ cho bên thứ ba nếu chưa được cấp có thẩm quyền cho phép.

3. Nhà thầu, đơn vị cung cấp dịch vụ bàn giao sản phẩm, tài liệu, dữ liệu, công cụ, mã nguồn hoặc quyền sử dụng, gói cài đặt, cấu hình, tài khoản quản trị, tài khoản tích hợp, API, tài liệu thiết kế, tài liệu quản trị, tài liệu người dùng, tài liệu kiểm thử, tài liệu an ninh mạng và tài sản kỹ thuật khác theo phạm vi hợp đồng, hình thức triển khai và hồ sơ được phê duyệt.

4. Trường hợp không chuyển giao mã nguồn hoặc cung cấp dưới hình thức dịch vụ, nhà thầu, đơn vị cung cấp dịch vụ phải bảo đảm quyền quản lý, khai thác, kết xuất, sao lưu, phục hồi, chuyển giao, trả về dữ liệu và xác nhận xoá dữ liệu khi chấm dứt dịch vụ theo hợp đồng hoặc thoả thuận được phê duyệt.

5. Đối với hệ thống có xử lý thông tin mật, nhà thầu, đơn vị cung cấp dịch vụ chỉ được tham gia khi đáp ứng điều kiện về nhân sự, tổ chức, địa điểm,

phương tiện, bảo mật và các yêu cầu khác theo quy định của Đảng, pháp luật của Nhà nước về bảo vệ bí mật nhà nước, cơ yếu, an ninh mạng, bảo mật thông tin.

6. Người sử dụng có trách nhiệm sử dụng tài khoản đúng mục đích, đúng thẩm quyền; bảo vệ thông tin đăng nhập; không chia sẻ, cho mượn tài khoản; không tự ý khai thác, kết xuất, sao chép, phát tán, sửa đổi hoặc xoá dữ liệu ngoài phạm vi được phân quyền; kịp thời thông báo khi phát hiện lỗi, sự cố, truy cập bất thường, dữ liệu sai lệch hoặc nguy cơ mất an ninh mạng, mất an toàn dữ liệu.

Điều 11. Bảng phân công trách nhiệm trong từng giai đoạn

1. Đối với từng hệ thống thông tin, chủ đầu tư hoặc đơn vị được giao quản lý nhiệm vụ, dự án chủ trì xác định trách nhiệm của các chủ thể theo từng giai đoạn. Nội dung phân công có thể lập thành Bảng phân công trách nhiệm hoặc được thể hiện trong đầu bài, phương án, hồ sơ thiết kế, hợp đồng, biên bản bàn giao hoặc tài liệu tương đương; trường hợp cần phê duyệt, xác nhận riêng thì thực hiện theo phân cấp.

2. Nội dung phân công trách nhiệm phải xác định tối thiểu chủ thể chủ trì, phối hợp, thẩm định hoặc tham gia ý kiến, phê duyệt, thực hiện, tiếp nhận vận hành, giám sát, kiểm tra và chủ thể chịu trách nhiệm cuối cùng theo từng nội dung.

3. Nội dung phân công trách nhiệm được lập hoặc cập nhật khi cần thiết tại các giai đoạn: đề xuất nhu cầu, xây dựng đầu bài; lập phương án; thiết kế, phát triển, cấu hình, mua sắm, thuê dịch vụ; kiểm thử, vận hành thử, nghiệm thu, bàn giao; vận hành, bảo trì, thay đổi, nâng cấp, xử lý sự cố; đánh giá định kỳ, dừng khai thác, chuyển giao, thay thế, thanh lý.

4. Đối với hệ thống dùng chung toàn hệ thống, hệ thống dùng chung theo ngành dọc, hệ thống có dữ liệu tập trung nhưng quản trị phân tán hoặc hệ thống liên thông với cơ quan, tổ chức khác trong hệ thống chính trị, Bảng phân công trách nhiệm phải phân định rõ trách nhiệm giữa cấp trên và cấp dưới, giữa cơ quan chủ quản hệ thống và chủ quản dữ liệu, giữa đơn vị vận hành và đơn vị cập nhật, khai thác dữ liệu.

5. Trường hợp một cơ quan, đơn vị hoặc cá nhân kiêm nhiệm nhiều vai trò, hồ sơ phải thể hiện rõ trách nhiệm theo từng vai trò; trường hợp phát sinh chồng lấn, khoảng trống hoặc xung đột trách nhiệm thì chủ đầu tư hoặc đơn vị được giao quản lý nhiệm vụ, dự án phải báo cáo cơ quan chủ quản hệ thống thông tin hoặc cấp có thẩm quyền xem xét, quyết định trước khi thực hiện bước tiếp theo.

Chương III
TIẾP NHẬN YÊU CẦU, XÂY DỰNG ĐẦU BÀI VÀ LẬP PHƯƠNG ÁN

Điều 12. Đề xuất nhu cầu và tiếp nhận yêu cầu

1. Khi có nhu cầu xây dựng mới, nâng cấp, mở rộng, mua sắm, thuê dịch vụ, tiếp nhận chuyển giao, sử dụng thử, sử dụng nền tảng dùng chung hoặc thay thế hệ thống thông tin, đơn vị chủ trì sử dụng lập Phiếu yêu cầu hoặc tài liệu đề xuất tương đương gửi chủ đầu tư hoặc đơn vị được giao quản lý nhiệm vụ, dự án để xem xét, xử lý theo thẩm quyền.

2. Phiếu yêu cầu hoặc tài liệu tương đương phải nêu rõ tên nhu cầu, căn cứ chính trị, pháp lý, nghiệp vụ, mục tiêu, phạm vi, đối tượng sử dụng, quy mô dự kiến, quy trình nghiệp vụ liên quan, điểm cần xử lý, dữ liệu dự kiến xử lý, nhu cầu tích hợp, yêu cầu vận hành liên tục, hình thức thực hiện, tiến độ và đầu mối phối hợp.

3. Phiếu yêu cầu hoặc tài liệu tương đương phải đánh giá sơ bộ khả năng sử dụng trực tiếp, cấu hình, kế thừa, dùng chung, tái sử dụng, tích hợp hoặc mở rộng lõi số dùng chung, thành phần dùng chung và hệ thống thông tin đã có; sự phù hợp với Khung Kiến trúc số trong các cơ quan Đảng và Kiến trúc số có liên quan; nguồn dữ liệu có thẩm quyền, khả năng kết nối, chia sẻ dữ liệu, tránh trùng lặp đầu tư và khả năng đáp ứng tiêu chuẩn, quy chuẩn kỹ thuật. Trường hợp đề xuất thành phần đặc thù phải nêu rõ khoảng trống mà thành phần dùng chung chưa đáp ứng và phương án tích hợp, hội tụ khi điều kiện thay đổi.

4. Chủ đầu tư hoặc đơn vị được giao quản lý nhiệm vụ, dự án có trách nhiệm tiếp nhận, kiểm tra tính đầy đủ, hợp lệ của Phiếu yêu cầu; phân công đầu mối xử lý; thông báo tiếp nhận hoặc yêu cầu bổ sung thông tin.

5. Trường hợp phát triển thử nghiệm, thử nghiệm có kiểm soát sản phẩm, dịch vụ, mô hình hoặc giải pháp công nghệ số, việc đề xuất, phê duyệt, tổ chức thử nghiệm, đánh giá, công nhận kết quả thử nghiệm và xử lý sau thử nghiệm thực hiện theo quy định của pháp luật về chuyển đổi số và hướng dẫn của cấp có thẩm quyền; không áp dụng trình tự đề xuất nhu cầu thông thường quy định tại các khoản 1, 2, 3 và 4 của Điều này, trừ trường hợp cấp có thẩm quyền yêu cầu.

Điều 13. Khảo sát nghiệp vụ, hiện trạng và dữ liệu

1. Căn cứ Phiếu yêu cầu đã được tiếp nhận, chủ đầu tư hoặc đơn vị được giao quản lý nhiệm vụ, dự án tổ chức khảo sát nghiệp vụ, dữ liệu, hệ thống thông tin, hạ tầng kỹ thuật, tích hợp, an ninh mạng và các điều kiện liên quan để làm cơ sở xây dựng đầu bài, lập phương án.

2. Trường hợp đã có đủ thông tin, tài liệu, dữ liệu, hồ sơ, báo cáo hoặc kết quả khảo sát trước đó làm cơ sở xây dựng đầu bài, lập phương án, có thể không tổ chức khảo sát mới hoặc chỉ khảo sát bổ sung đối với nội dung còn thiếu; việc này phải được thể hiện trong hồ sơ.

3. Nội dung khảo sát phải xác định được quy trình nghiệp vụ, hồ sơ, biểu mẫu, nhóm người dùng, vai trò, quyền hạn, điểm cần cải tiến và yêu cầu chuẩn hoá trước khi số hoá; đồng thời ghi nhận danh mục dữ liệu, nguồn dữ liệu có thẩm quyền, nơi tạo lập và chủ thể chịu trách nhiệm xác lập giá trị gốc, chủ thể cập nhật, cấu trúc, chất lượng, dữ liệu chủ, dữ liệu tham chiếu, dữ liệu dùng chung, dữ liệu kế thừa, dữ liệu cần làm sạch, chuẩn hoá, đối soát, dữ liệu mật hoặc dữ liệu nhạy cảm nếu có.

4. Đối với hệ thống, hạ tầng kỹ thuật và an ninh mạng, nội dung khảo sát phải đánh giá các hệ thống liên quan, chức năng nghiệp vụ, dữ liệu xử lý, đối tượng sử dụng, đối tượng vận hành, đối tượng phục vụ, yêu cầu tích hợp, tài khoản, phân quyền, nhật ký, sao lưu, phục hồi, giám sát, cấp độ của hệ thống thông tin, rủi ro an ninh mạng và khả năng phụ thuộc, tác động dây chuyền giữa các hệ thống; trường hợp hệ thống có yêu cầu mô hình kiến trúc hoặc xử lý thông tin mật thì bổ sung các nội dung về lớp nghiệp vụ, ứng dụng, dữ liệu, hạ tầng, điểm phát sinh thông tin mật, môi trường mạng, thiết bị, nhân sự, cơ yếu và bảo mật.

5. Kết quả khảo sát phải được lập thành Biên bản khảo sát hoặc Báo cáo khảo sát, có xác nhận của các bên tham gia theo phạm vi trách nhiệm.

Điều 14. Xây dựng, thẩm định và phê duyệt đầu bài

1. Trên cơ sở Phiếu yêu cầu hoặc tài liệu tương đương, kết quả khảo sát và tài liệu liên quan, chủ đầu tư hoặc đơn vị được giao quản lý nhiệm vụ, dự án chủ trì xây dựng đầu bài, có sự tham gia của đơn vị chủ trì sử dụng, đơn vị chuyên trách chuyển đổi số, an ninh mạng, cơ yếu, chủ quản dữ liệu, đơn vị quản trị dữ liệu, đơn vị vận hành và các đơn vị liên quan.

2. Đầu bài phải mô tả tối thiểu mục tiêu, phạm vi, đối tượng sử dụng, quy trình nghiệp vụ, yêu cầu chức năng, yêu cầu phi chức năng, yêu cầu dữ liệu, yêu cầu tích hợp, yêu cầu an ninh mạng, yêu cầu bảo vệ bí mật nhà nước, yêu cầu vận hành, yêu cầu kiểm thử, nghiệm thu, bàn giao và tiêu chí đánh giá kết quả.

3. Đối với nội dung dữ liệu, đầu bài phải xác định dữ liệu đầu vào, dữ liệu đầu ra, dữ liệu nghiệp vụ, dữ liệu chủ, dữ liệu tham chiếu, dữ liệu dùng chung, dữ liệu kế thừa, chủ quản dữ liệu, nguồn dữ liệu có thẩm quyền, nơi tạo lập, đơn

vị cập nhật, đơn vị khai thác, phạm vi xử lý, mục đích xử lý, thời hạn lưu trữ, yêu cầu làm sạch, chuẩn hoá, đối soát và trách nhiệm quản lý chất lượng dữ liệu.

4. Đầu bài phải được đánh giá sơ bộ về sự phù hợp với Khung Kiến trúc số trong các cơ quan Đảng và Kiến trúc số có liên quan; khả năng sử dụng lõi số dùng chung, thành phần dùng chung, nguồn dữ liệu có thẩm quyền; kiến trúc dữ liệu, tiêu chuẩn kết nối, tích hợp, chia sẻ dữ liệu và yêu cầu an ninh mạng.

5. Đối với hệ thống có xử lý thông tin mật, dữ liệu cá nhân hoặc dữ liệu nội bộ hạn chế truy cập, đầu bài phải xác định rõ loại thông tin, loại dữ liệu, phạm vi xử lý, thẩm quyền tiếp cận, yêu cầu bảo vệ, yêu cầu nhật ký, yêu cầu sao lưu, phục hồi, thu hồi, tiêu huỷ và điều kiện chia sẻ.

6. Đầu bài sau khi hoàn thiện phải được lấy ý kiến các đơn vị liên quan theo phạm vi trách nhiệm; nội dung tiếp thu, giải trình phải được thể hiện trong hồ sơ. Đầu bài hoặc tài liệu yêu cầu tương đương được phê duyệt hoặc xác nhận theo thẩm quyền là căn cứ để lập phương án xây dựng, triển khai, thiết kế, kiểm thử, vận hành thử, nghiệm thu và bàn giao.

Điều 15. Đánh giá tuân thủ Kiến trúc số

1. Việc xây dựng, nâng cấp, mở rộng, mua sắm, thuê dịch vụ, tiếp nhận chuyển giao, thay đổi lớn hoặc thay thế hệ thống thông tin phải được đánh giá sự phù hợp với Khung Kiến trúc số trong các cơ quan Đảng và các tài liệu Kiến trúc số có liên quan theo mức độ, phạm vi và nhóm áp dụng của hệ thống.

2. Nội dung đánh giá tập trung vào khả năng truy vết từ yêu cầu nghiệp vụ, năng lực cần hình thành đến hệ thống; mức độ kế thừa lõi số dùng chung và thành phần dùng chung; ranh giới dùng chung - chuyên ngành - đặc thù; nguồn dữ liệu có thẩm quyền; dữ liệu, ứng dụng, nền tảng, hạ tầng, tích hợp, kênh tương tác, quản trị, vận hành, an toàn, an ninh mạng, cơ yếu, bảo mật, bảo vệ dữ liệu; khả năng mở rộng, thay thế, chuyển giao, quản lý vòng đời và tránh đầu tư trùng lặp.

3. Việc đánh giá tuân thủ kiến trúc được thực hiện tại các giai đoạn phù hợp, gồm đề xuất nhu cầu, xây dựng đầu bài, lập phương án, xây dựng hoặc cập nhật Kiến trúc số giải pháp khi có yêu cầu, thiết kế, kiểm thử, nghiệm thu, bàn giao và khi có thay đổi lớn về nghiệp vụ, kiến trúc, dữ liệu, tích hợp, cấp độ của hệ thống thông tin hoặc phạm vi vận hành.

4. Trường hợp chưa đáp ứng đầy đủ yêu cầu kiến trúc nhưng có căn cứ nghiệp vụ và cần triển khai do yêu cầu cấp thiết thì được xem xét như ngoại lệ

kiến trúc. Hồ sơ phải nêu rõ nội dung chưa tuân thủ, lý do, phạm vi, chủ thể chịu trách nhiệm, đánh giá rủi ro, biện pháp kiểm soát, thời hạn áp dụng, điều kiện rà soát và lộ trình tích hợp, hội tụ, khắc phục hoặc kết thúc; ngoại lệ không được sử dụng để hợp thức hoá đầu tư trùng lặp và phải được cấp có thẩm quyền xem xét, quyết định.

5. Kết quả đánh giá tuân thủ, nội dung chưa tuân thủ, ngoại lệ kiến trúc và tình trạng khắc phục phải được ghi nhận trong hồ sơ của hệ thống; trường hợp làm thay đổi Kiến trúc số cấp cơ quan, Kiến trúc số chuyên ngành hoặc Kiến trúc số trong các cơ quan Đảng tỉnh, thành phố thì phải cập nhật tài liệu kiến trúc có liên quan theo quy định.

Điều 16. Xử lý khi nghiệp vụ thay đổi

1. Khi nghiệp vụ của đơn vị chủ trì sử dụng thay đổi do sửa đổi, bổ sung quy định của Đảng, pháp luật của Nhà nước, thay đổi quy trình nội bộ, thay đổi cơ cấu tổ chức, phát sinh nghiệp vụ mới hoặc bãi bỏ nghiệp vụ hiện có làm cho hệ thống thông tin không còn đáp ứng yêu cầu, đơn vị chủ trì sử dụng có trách nhiệm thông báo bằng văn bản cho chủ đầu tư hoặc đơn vị được giao quản lý nhiệm vụ, dự án.

2. Chủ đầu tư hoặc đơn vị được giao quản lý nhiệm vụ, dự án chủ trì, phối hợp với đơn vị chủ trì sử dụng, đơn vị vận hành, chủ quản dữ liệu và các đơn vị liên quan đánh giá tác động của thay đổi.

3. Thay đổi được phân loại thành: thay đổi cấu hình; nâng cấp, mở rộng; xây dựng mới hoặc thay thế. Việc phân loại căn cứ mức độ thay đổi về nghiệp vụ, mã nguồn, kiến trúc, công nghệ, mô hình nghiệp vụ, dữ liệu hoặc cấp độ của hệ thống thông tin.

4. Việc đánh giá tác động phải xem xét yêu cầu nghiệp vụ, năng lực số, sự phù hợp với Khung và Kiến trúc số có liên quan, lõi số dùng chung, dữ liệu, nguồn dữ liệu có thẩm quyền, tích hợp, quyền truy cập, phân quyền, nhật ký, cấp độ của hệ thống thông tin, thông tin mật, dữ liệu cá nhân, dữ liệu hạn chế truy cập, vận hành, chi phí, tiến độ, đào tạo, hỗ trợ người dùng và khả năng quay lui khi thay đổi không đạt yêu cầu.

5. Kết quả đánh giá, phân loại thay đổi và phương án xử lý phải được lập thành hồ sơ, trình cấp có thẩm quyền phê duyệt hoặc xác nhận theo phân cấp trước khi thực hiện. Thay đổi lớn ảnh hưởng đến kiến trúc mục tiêu, ranh giới dùng chung - đặc thù, nguồn dữ liệu có thẩm quyền, tích hợp hoặc lộ trình chuyển đổi phải đồng thời cập nhật Kiến trúc số giải pháp và tài liệu Kiến trúc

số có liên quan; trong thời gian xử lý thay đổi, các đơn vị liên quan áp dụng phương án nghiệp vụ tạm thời để bảo đảm hoạt động không bị gián đoạn.

Điều 17. Lập, phê duyệt và điều chỉnh phương án xây dựng, triển khai

1. Trên cơ sở đầu bài đã được phê duyệt, chủ đầu tư hoặc đơn vị được giao quản lý nhiệm vụ, dự án chủ trì lập phương án xây dựng, triển khai hệ thống thông tin.

2. Phương án xây dựng, triển khai phải xác định rõ thiết kế tổng thể, thiết kế chi tiết hoặc tài liệu tương đương phù hợp với hình thức triển khai; mô hình nghiệp vụ, mô hình dữ liệu, mô hình ứng dụng, mô hình tích hợp, mô hình hạ tầng, mô hình an ninh mạng và điều kiện vận hành, nghiệm thu, bàn giao. Ưu tiên sử dụng nền tảng, hệ thống, thành phần dùng chung đáp ứng yêu cầu; không đầu tư, thuê dịch vụ hoặc phát triển hệ thống, phần mềm trùng lặp, phân tán. Đối với hệ thống thông tin, dịch vụ công nghệ số có quy mô, tính chất và mức độ phức tạp không lớn, phương án xây dựng, triển khai phải bảo đảm tinh gọn, rõ đầu mối và trách nhiệm; hạn chế việc phân chia, tổ chức thực hiện làm phát sinh không cần thiết nhiều đầu mối cung cấp sản phẩm, dịch vụ, gây khó khăn cho việc tích hợp, quản lý chất lượng, bảo đảm an ninh mạng, vận hành, bảo hành, bảo trì và xác định trách nhiệm, phù hợp với quy định của pháp luật về đầu tư, đấu thầu, mua sắm và quy định có liên quan.

3. Đối với phần mềm thương mại, nền tảng dùng chung, dịch vụ công nghệ số hoặc hệ thống có xử lý thông tin mật, dữ liệu nhạy cảm, phương án phải làm rõ điều kiện sử dụng, quyền dữ liệu, trách nhiệm nhà cung cấp, môi trường triển khai, kiểm soát truy cập, bảo mật, cơ yếu, sao lưu, phục hồi và điều kiện tham gia của nhà thầu.

4. Phương án xây dựng, triển khai được phê duyệt theo thẩm quyền là căn cứ để tổ chức thiết kế, phát triển, cấu hình, mua sắm, thuê dịch vụ, kiểm thử, nghiệm thu, bàn giao và đưa vào vận hành chính thức. Khi phát sinh thay đổi ảnh hưởng đến phạm vi, kiến trúc, công nghệ, dữ liệu, tích hợp, cấp độ của hệ thống thông tin, tiến độ, chi phí hoặc phương án vận hành, phải lập hồ sơ điều chỉnh phương án và trình cấp có thẩm quyền xem xét, quyết định.

5. Việc lập, thẩm định, phê duyệt hồ sơ xác định cấp độ và phương án bảo vệ an ninh mạng theo cấp độ được thực hiện theo quy định của Đảng, pháp luật của Nhà nước và phân cấp có liên quan; các điều kiện bắt buộc về an ninh mạng phải được hoàn thành trước khi hệ thống được đưa vào vận hành chính thức.

6. Hình thức, bước thiết kế và hồ sơ thiết kế hệ thống thông tin được xác định theo quy định pháp luật hiện hành, phù hợp với quy mô, tính chất, mức độ phức tạp và hình thức triển khai. Hồ sơ thiết kế phải làm rõ kiến trúc, chức năng, dữ liệu, tích hợp, hạ tầng, an ninh mạng, an ninh dữ liệu, kiểm thử, nghiệm thu, vận hành và bảo trì phù hợp với nhiệm vụ, dự án hoặc hoạt động triển khai.

Điều 18. Kiến trúc số giải pháp, mô hình kiến trúc và ứng dụng trí tuệ nhân tạo

1. Nhiệm vụ, dự án, hệ thống thông tin, cơ sở dữ liệu, nền tảng số hoặc hạ tầng số có quy mô người dùng lớn, liên quan đến nhiều cấp, nhiều cơ quan, nhiều hệ thống khác hoặc có yêu cầu cao về an toàn, an ninh mạng, bảo mật, bảo vệ dữ liệu phải xây dựng Kiến trúc số giải pháp phù hợp với Khung và các tài liệu Kiến trúc số có liên quan.

2. Kiến trúc số giải pháp phải làm rõ tối thiểu nghiệp vụ và năng lực cần đáp ứng; dữ liệu và nguồn dữ liệu có thẩm quyền; ứng dụng, nền tảng, hạ tầng, tích hợp, API hoặc dịch vụ dữ liệu; ranh giới dùng chung - đặc thù; định danh, phân quyền; an toàn, an ninh mạng, cơ yếu, bảo mật, bảo vệ dữ liệu; vận hành, mức dịch vụ, chuyển đổi và vòng đời. Nội dung Kiến trúc số giải pháp có thể được tích hợp trong phương án xây dựng, triển khai hoặc hồ sơ thiết kế nếu bảo đảm đầy đủ nội dung và khả năng truy vết theo hướng dẫn của Văn phòng Trung ương Đảng.

3. Đối với các hệ thống không thuộc trường hợp quy định tại khoản 1 Điều này, phương án xây dựng, triển khai vẫn phải xác định mô hình kiến trúc phù hợp với quy mô, tính chất nhiệm vụ, mức độ quan trọng, cấp độ của hệ thống thông tin, mức độ mật, phạm vi dùng chung, phạm vi kết nối, chia sẻ dữ liệu và hình thức triển khai của hệ thống.

4. Đối với hệ thống quan trọng, hệ thống trọng yếu, hệ thống dùng chung, hệ thống có xử lý thông tin mật, hệ thống có dữ liệu tập trung hoặc có kết nối, chia sẻ dữ liệu rộng, phương án phải thể hiện mô hình tổng thể, mô hình lô-gic, mô hình vật lý hoặc tài liệu tương đương; làm rõ lớp người dùng, nghiệp vụ, ứng dụng, dữ liệu, nền tảng, hạ tầng công nghệ số, an ninh mạng và quan hệ tích hợp với các hệ thống liên quan. Đối với hệ thống quy mô nhỏ, nội bộ, ít rủi ro, có thể áp dụng mô hình rút gọn nhưng vẫn phải mô tả được yêu cầu nghiệp vụ, dữ liệu xử lý, thành phần chính, môi trường triển khai, phân quyền, sao lưu, phục hồi, yêu cầu cơ bản về an ninh mạng và điều kiện nghiệm thu.

5. Trường hợp hệ thống thông tin có ứng dụng trí tuệ nhân tạo, phương án phải xác định rõ mục đích, phạm vi sử dụng, loại dữ liệu được xử lý, dữ liệu huấn luyện, dữ liệu kiểm thử, cơ chế kiểm soát dữ liệu đầu vào, đầu ra, trách nhiệm giám sát của con người, nhật ký xử lý khi cần thiết và biện pháp phòng ngừa sai lệch, lạm dụng, lộ lọt dữ liệu hoặc sử dụng vượt phạm vi được phê duyệt. Việc ứng dụng trí tuệ nhân tạo đối với thông tin mật, dữ liệu cá nhân, dữ liệu cá nhân nhạy cảm, dữ liệu nội bộ nhạy cảm, dữ liệu hạn chế truy cập chỉ được thực hiện khi có biện pháp bảo vệ phù hợp và được cấp có thẩm quyền cho phép.

Chương IV
DỮ LIỆU, AN NINH MẠNG VÀ AN NINH DỮ LIỆU

Điều 19. Quản lý dữ liệu, dữ liệu kế thừa, kết nối và chia sẻ dữ liệu

1. Dữ liệu trong hệ thống thông tin phải được quản lý như một thành phần độc lập, có chủ quản dữ liệu, đơn vị quản trị dữ liệu, mục đích xử lý, phạm vi xử lý, trách nhiệm cập nhật, trách nhiệm khai thác, trách nhiệm chia sẻ và trách nhiệm bảo vệ rõ ràng.

2. Yêu cầu dữ liệu phải được xác định từ giai đoạn đề xuất nhu cầu, khảo sát, xây dựng đầu bài, lập phương án và được cập nhật trong quá trình thiết kế, triển khai, kiểm thử, nghiệm thu, bàn giao, vận hành, thay đổi, nâng cấp, thay thế hoặc dừng khai thác.

3. Hồ sơ dữ liệu phải thể hiện tối thiểu danh mục dữ liệu, chủ quản dữ liệu, nguồn dữ liệu có thẩm quyền, nơi tạo lập, đơn vị cập nhật, đơn vị khai thác, cấu trúc dữ liệu, chuẩn dữ liệu, mã định danh, dữ liệu chủ, dữ liệu tham chiếu, dữ liệu dùng chung, dữ liệu kế thừa, dữ liệu cần chia sẻ, dữ liệu hạn chế truy cập, dữ liệu cá nhân, dữ liệu mật nếu có. Đối với mỗi dữ liệu trọng yếu phải xác định hệ thống hoặc nguồn có thẩm quyền và cơ chế xử lý sai khác; trong cùng một ngữ cảnh chỉ một nguồn được xác lập giá trị gốc cho một thuộc tính dữ liệu.

4. Dữ liệu phải được tạo lập một lần tại nguồn có thẩm quyền, bảo đảm đúng, đủ, sạch, cập nhật và có khả năng chia sẻ, tái sử dụng theo phân quyền. Ưu tiên khai thác dữ liệu dùng chung thông qua API, dịch vụ dữ liệu hoặc cơ chế đồng bộ được kiểm soát; không hình thành lâu dài các nguồn dữ liệu song song, độc lập và không đối soát.

5. Đối với hệ thống thông tin nâng cấp, thay thế, tích hợp, chuyển đổi hoặc tiếp nhận dữ liệu từ hệ thống cũ, phải có phương án chuyển đổi, làm sạch,

chuẩn hoá và đối soát dữ liệu kế thừa trước khi nghiệm thu, bàn giao hoặc đưa vào vận hành chính thức.

6. Việc kết nối, tích hợp, chia sẻ dữ liệu giữa hệ thống thông tin trong các cơ quan Đảng và với cơ quan, tổ chức khác trong hệ thống chính trị phải đúng mục đích, đúng thẩm quyền, đúng phạm vi, tối thiểu cần thiết và có khả năng truy vết.

7. Hồ sơ kết nối, tích hợp, chia sẻ dữ liệu phải làm rõ hệ thống cung cấp dữ liệu, hệ thống khai thác dữ liệu, loại dữ liệu, mục đích khai thác, phạm vi chia sẻ, tần suất, phương thức kết nối, phân quyền, nhật ký, trách nhiệm vận hành, trách nhiệm xử lý sự cố và thời hạn hiệu lực.

8. Dữ liệu mật, dữ liệu cá nhân, dữ liệu nội bộ hạn chế truy cập trong quá trình chuyển đổi, kiểm thử, đối soát, kết nối, chia sẻ phải được bảo vệ theo đúng quy định; không sử dụng dữ liệu gốc trong môi trường phát triển, kiểm thử, trình diễn nếu chưa được cấp có thẩm quyền cho phép và chưa có biện pháp bảo vệ phù hợp. Dữ liệu và tài nguyên thông tin thuộc phạm vi quản lý của cơ quan Đảng phải được lưu trữ, xử lý trên hạ tầng, môi trường đáp ứng yêu cầu về an ninh mạng, bảo vệ bí mật nhà nước, bảo vệ dữ liệu và được cấp có thẩm quyền cho phép theo quy định. Việc xây dựng, thuê dịch vụ, vận hành hoặc sử dụng nền tảng của nhà cung cấp phải bảo đảm cơ quan chủ quản duy trì quyền quản lý, kiểm soát đối với hệ thống và dữ liệu thuộc phạm vi quản lý; có khả năng truy cập, khai thác, kết xuất, sao lưu, phục hồi, chuyển giao dữ liệu và duy trì hoặc khôi phục hoạt động của hệ thống trong suốt vòng đời, hạn chế phụ thuộc vào nhà cung cấp.

Điều 20. An ninh mạng, thông tin mật, dữ liệu cá nhân và dữ liệu hạn chế truy cập

1. Yêu cầu về cấp độ của hệ thống thông tin phải được nhận diện từ giai đoạn đề xuất nhu cầu, làm rõ trong đầu bài và phương án xây dựng, triển khai. Việc lập, thẩm định, phê duyệt hồ sơ xác định cấp độ và phương án bảo vệ an ninh mạng theo cấp độ thực hiện theo quy định của Đảng, pháp luật của Nhà nước; phải bảo đảm hoàn thành các điều kiện bắt buộc trước khi đưa hệ thống vào vận hành chính thức.

2. Hồ sơ xác định cấp độ của hệ thống thông tin, phương án bảo vệ an ninh mạng theo cấp độ, quy chế bảo vệ an ninh mạng và các tài liệu liên quan được lập, thẩm định, phê duyệt theo quy định của Đảng, pháp luật của Nhà nước

về bảo vệ an ninh mạng đối với hệ thống thông tin theo cấp độ, trong đó thực hiện đúng thẩm quyền, trình tự, thủ tục đối với hệ thống cấp độ 1, 2, 3, 4, 5 và hệ thống thông tin quan trọng về an ninh quốc gia.

3. Đối với hệ thống cấp độ 4, cấp độ 5, hệ thống thông tin quan trọng về an ninh quốc gia, hệ thống có sử dụng cơ yếu, mật mã hoặc có yếu tố quốc phòng, an ninh, hồ sơ xác định cấp độ, phương án bảo vệ an ninh mạng và việc thẩm định, phê duyệt phải được gửi lấy ý kiến, thẩm định hoặc phối hợp với Bộ Công an, Bộ Quốc phòng, Ban Cơ yếu Chính phủ hoặc cơ quan có thẩm quyền theo quy định.

4. Chủ quản hệ thống thông tin có trách nhiệm tổ chức đánh giá rủi ro an ninh mạng khi xác định cấp độ lần đầu; khi có thay đổi chức năng, phạm vi phục vụ, đối tượng sử dụng, loại thông tin xử lý hoặc kết nối, chia sẻ dữ liệu với hệ thống khác; khi xảy ra sự cố an ninh mạng nghiêm trọng hoặc khi có yêu cầu của cơ quan có thẩm quyền. Kết quả đánh giá rủi ro là căn cứ xác định, điều chỉnh cấp độ, lựa chọn biện pháp bảo vệ và hoàn thiện phương án bảo vệ an ninh mạng.

5. Đối với dữ liệu cá nhân, dữ liệu hạn chế truy cập, phải xác định mục đích xử lý, phạm vi xử lý, chủ thể được tiếp cận, phân quyền, nhật ký truy cập, thời hạn lưu trữ, phương án bảo vệ, phương án xử lý khi có sự cố và điều kiện chia sẻ.

6. Hệ thống có xử lý thông tin mật phải được thiết kế, triển khai, vận hành theo nguyên tắc phân vùng, phân lớp, kiểm soát truy cập chặt chẽ, tách biệt phù hợp giữa vùng xử lý thông tin mật và vùng không xử lý thông tin mật; không kết nối, chia sẻ, truyền đưa thông tin mật qua môi trường không đáp ứng yêu cầu bảo vệ.

7. Nhà thầu, đơn vị cung cấp dịch vụ và nhân sự tham gia xây dựng, triển khai, kiểm thử, vận hành, bảo trì hệ thống thông tin phải được quản lý, kiểm soát theo yêu cầu về an ninh mạng, bảo mật thông tin, bảo vệ bí mật nhà nước, bảo vệ dữ liệu và quy định của cấp có thẩm quyền. Việc cấp quyền truy cập hệ thống, nhất là đối với tài khoản quản trị, tài khoản đặc quyền, phải bảo đảm đúng đối tượng, đúng phạm vi, đúng mục đích, trong thời hạn cần thiết và theo nguyên tắc quyền tối thiểu; được phê duyệt, giám sát, ghi nhật ký, định kỳ rà

soát và thu hồi kịp thời khi không còn nhu cầu hoặc khi nhân sự thay đổi nhiệm vụ, chấm dứt tham gia.

Điều 21. Kiểm tra, đánh giá, kiểm thử an ninh mạng và giám sát tập trung

1. Trước khi nghiệm thu, bàn giao đưa vào vận hành chính thức, hệ thống thông tin phải được kiểm tra, đánh giá, kiểm thử an ninh mạng phù hợp với cấp độ, mức độ quan trọng, tính chất thông tin xử lý và phạm vi kết nối, chia sẻ dữ liệu.

2. Nội dung kiểm tra, đánh giá, kiểm thử an ninh mạng gồm tối thiểu kiểm tra cấu hình, phân quyền, xác thực, nhật ký, lỗ hổng, điểm yếu, khả năng chống truy cập trái phép, an ninh dữ liệu, an toàn dữ liệu, an toàn tích hợp, sao lưu, phục hồi, khả năng xử lý sự cố; đồng thời xem xét mức độ tuân thủ, hiệu quả của biện pháp bảo vệ an ninh mạng, quản lý rủi ro an ninh mạng và yêu cầu của hồ sơ xác định cấp độ đã được phê duyệt.

3. Đối với hệ thống quan trọng, trọng yếu, hệ thống có xử lý thông tin mật, hệ thống dùng chung quy mô lớn hoặc hệ thống có kết nối, chia sẻ dữ liệu rộng, việc kiểm tra, đánh giá, kiểm thử an ninh mạng phải được thực hiện bởi đơn vị có năng lực phù hợp và độc lập với đơn vị phát triển trong phạm vi cần thiết.

4. Phát hiện về lỗ hổng, điểm yếu, cấu hình sai, phân quyền sai, rủi ro dữ liệu, rủi ro tích hợp hoặc rủi ro vận hành phải được phân loại, xử lý, kiểm tra lại và lập hồ sơ trước khi nghiệm thu hoặc đưa vào vận hành chính thức.

5. Đối với hệ thống trọng yếu, hệ thống có xử lý thông tin mật, hệ thống dùng chung quy mô lớn hoặc hệ thống có kết nối, chia sẻ dữ liệu rộng, phải có phương án giám sát an ninh mạng tập trung, cảnh báo, tiếp nhận, xử lý sự cố và báo cáo theo quy định.

6. Việc kiểm tra, đánh giá an ninh mạng định kỳ hoặc đột xuất có thể bao gồm kiểm tra tuân thủ, đánh giá hiệu quả biện pháp bảo vệ, dò quét, phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm tấn công hoặc kiểm thử xâm nhập theo phương pháp phù hợp với cấp độ, mức độ rủi ro, tính chất dữ liệu và phạm vi kết nối của hệ thống.

Chương V
TRIỂN KHAI, KIỂM THỬ, VẬN HÀNH THỬ, NGHIỆM THU VÀ BÀN GIAO

Điều 22. Tổ chức triển khai và quản lý kỹ thuật

1. Việc triển khai hệ thống thông tin được thực hiện theo đầu bài, phương án xây dựng, triển khai, thiết kế, hợp đồng, hồ sơ yêu cầu, tiêu chuẩn kỹ thuật, yêu cầu dữ liệu, yêu cầu an ninh mạng và các nội dung đã được phê duyệt.

2. Hoạt động triển khai bao gồm thiết kế chi tiết, phát triển, cấu hình, mua sắm, cài đặt, tích hợp, chuyển đổi dữ liệu, kiểm thử, đào tạo, chuyển giao, vận hành thử và các hoạt động khác phù hợp với hình thức thực hiện.

3. Chủ đầu tư hoặc đơn vị được giao quản lý nhiệm vụ, dự án tổ chức theo dõi, giám sát chất lượng, tiến độ, phạm vi, dữ liệu, an ninh mạng, rủi ro, phát sinh và việc tuân thủ phương án được phê duyệt.

4. Môi trường phát triển, kiểm thử, vận hành thử và vận hành chính thức phải được quản lý, phân tách phù hợp; việc can thiệp trực tiếp vào môi trường vận hành chính thức chỉ thực hiện khi được phê duyệt hoặc trong trường hợp khẩn cấp theo quy trình xử lý sự cố và phải có biện pháp kiểm soát rủi ro.

5. Đối với phần mềm được phát triển mới, nâng cấp, mở rộng hoặc cấu hình theo yêu cầu riêng, mã nguồn, gói cài đặt, cấu hình, phiên bản, tài liệu thiết kế, tài liệu biên dịch, tài liệu triển khai và tài liệu quản trị phải được quản lý, lưu trữ, bàn giao theo phạm vi hợp đồng và hồ sơ được phê duyệt.

6. Đối với phần mềm thương mại, dịch vụ công nghệ số, nền tảng dùng chung hoặc trường hợp không bàn giao mã nguồn, hồ sơ phải làm rõ quyền sử dụng, quyền cấu hình, quyền quản trị, quyền truy cập dữ liệu, quyền kết xuất dữ liệu, quyền sao lưu, quyền chuyển đổi, quyền trả về và xoá dữ liệu khi chấm dứt sử dụng.

Điều 23. Kiểm thử và vận hành thử

1. Hệ thống thông tin phải được kiểm thử trước khi nghiệm thu, bàn giao đưa vào vận hành chính thức. Phạm vi kiểm thử được xác định theo đầu bài, phương án xây dựng, triển khai, mức độ quan trọng, cấp độ của hệ thống thông tin, phạm vi dữ liệu, phạm vi tích hợp và hình thức triển khai.

2. Kiểm thử phải bao gồm các nội dung phù hợp: chức năng; dữ liệu; tích hợp; hiệu năng, tải, khả năng mở rộng, khả năng sẵn sàng; sao lưu, phục hồi; an ninh mạng và khả năng xử lý lỗi giữa các hệ thống liên quan.

3. Sau khi kiểm thử đạt yêu cầu, hệ thống thông tin được tổ chức vận hành thử trong phạm vi, thời gian, môi trường và điều kiện do phương án xây dựng, triển khai xác định.

4. Vận hành thử nhằm đánh giá khả năng đáp ứng yêu cầu nghiệp vụ thực tế, tính ổn định, hiệu năng, dữ liệu, phân quyền, tích hợp, hỗ trợ người dùng, vận hành, sao lưu, phục hồi, an ninh mạng và khả năng xử lý sự cố.

5. Đơn vị chủ trì sử dụng chủ trì đánh giá mức độ đáp ứng yêu cầu nghiệp vụ; hệ thống dùng chung, hệ thống theo ngành dọc, hệ thống nhiều người dùng hoặc hệ thống có kết nối, chia sẻ dữ liệu rộng phải có sự tham gia đại diện các nhóm người dùng, đơn vị cập nhật dữ liệu, đơn vị khai thác dữ liệu và đơn vị vận hành.

6. Kết quả kiểm thử, vận hành thử phải được lập thành biên bản hoặc báo cáo, nêu rõ phạm vi, kịch bản, dữ liệu kiểm thử, kết quả đạt, chưa đạt, lỗi, biện pháp khắc phục và kết quả kiểm tra lại; đây là thành phần của hồ sơ nghiệm thu, bàn giao.

7. Đối với hệ thống thuộc nhóm áp dụng đầy đủ, hệ thống quan trọng, trọng yếu, hệ thống có xử lý thông tin mật, dữ liệu cá nhân nhạy cảm, dữ liệu nội bộ nhạy cảm, dữ liệu hạn chế truy cập hoặc hệ thống có kết nối, chia sẻ dữ liệu rộng, việc kiểm thử độc lập, kiểm thử tích hợp, kiểm thử an ninh mạng và vận hành thử tại đơn vị thụ hưởng được thực hiện theo quy định của pháp luật về chuyển đổi số, quy định về quản lý chất lượng và phạm vi được cấp có thẩm quyền phê duyệt.

Điều 24. Nghiệm thu hệ thống thông tin và dịch vụ công nghệ số

1. Việc nghiệm thu được thực hiện theo nguyên tắc đối chiếu sản phẩm, dịch vụ với đầu bài, phương án, yêu cầu nghiệp vụ, yêu cầu dữ liệu, yêu cầu tích hợp, yêu cầu an ninh mạng, an ninh dữ liệu, an toàn dữ liệu, yêu cầu vận hành, tiêu chí nghiệm thu và hồ sơ bàn giao.

2. Nghiệm thu kỹ thuật do chủ đầu tư hoặc đơn vị được giao quản lý nhiệm vụ, dự án chủ trì, có sự tham gia của đơn vị chuyên trách chuyển đổi số, an ninh mạng, cơ yếu, đơn vị vận hành, đơn vị chủ trì sử dụng, nhà thầu và các đơn vị liên quan theo phạm vi trách nhiệm.

3. Nghiệm thu sử dụng do đơn vị chủ trì sử dụng chủ trì hoặc xác nhận theo phân công, nhằm đánh giá mức độ đáp ứng yêu cầu nghiệp vụ, quy trình, biểu mẫu, dữ liệu, báo cáo, thống kê, tra cứu, phân quyền, trải nghiệm sử dụng, kết quả đào tạo và khả năng khai thác thực tế.

4. Chủ quản dữ liệu hoặc đơn vị được giao trách nhiệm về dữ liệu phải xác nhận kết quả dữ liệu thuộc phạm vi quản lý trước khi nghiệm thu đối với hệ thống có xử lý, chuyển đổi, tích hợp, chia sẻ hoặc khai thác dữ liệu nghiệp vụ.

5. Đối với dịch vụ công nghệ số, phần mềm thương mại, nền tảng dùng chung hoặc dịch vụ điện toán đám mây, nghiệm thu phải căn cứ cả điều kiện dịch vụ, quyền sử dụng, quyền dữ liệu, chất lượng dịch vụ, an ninh mạng, bảo mật thông tin, khả năng kết xuất dữ liệu, sao lưu, phục hồi, chuyển giao, trả về và xoá dữ liệu khi chấm dứt dịch vụ.

6. Chưa tổ chức nghiệm thu hoặc đưa vào vận hành chính thức nếu chưa làm rõ quyền dữ liệu, chưa đáp ứng yêu cầu bảo mật thông tin, an ninh mạng, bảo vệ dữ liệu, hoặc chưa hoàn thành các điều kiện bắt buộc về kiểm thử, nghiệm thu sử dụng, bàn giao và phương án vận hành.

7. Đối với dịch vụ thuê, nghiệm thu dịch vụ là hoạt động định kỳ trong suốt thời hạn hợp đồng, được thực hiện theo kỳ nghiệm thu, chất lượng dịch vụ, cam kết mức dịch vụ, kết quả xử lý yêu cầu, sự cố, bảo mật thông tin, an ninh mạng, an ninh dữ liệu, an toàn dữ liệu và quyền dữ liệu được quy định trong hợp đồng hoặc thoả thuận dịch vụ; không chỉ thực hiện một lần tại thời điểm kết thúc triển khai hoặc bàn giao ban đầu.

Điều 25. Bàn giao đưa vào vận hành chính thức và hồ sơ hoàn thành

1. Sau khi nghiệm thu đạt yêu cầu, chủ đầu tư hoặc đơn vị được giao quản lý nhiệm vụ, dự án chủ trì tổ chức bàn giao hệ thống thông tin cho cơ quan chủ quản hệ thống thông tin, đơn vị vận hành, đơn vị chủ trì sử dụng và các đơn vị liên quan theo phạm vi trách nhiệm.

2. Hồ sơ bàn giao, hồ sơ hoàn thành được lập thành danh mục, lưu trữ tập trung, phân quyền truy cập và bảo vệ theo mức độ mật, mức độ nhạy cảm. Hồ sơ phải đủ để phục vụ vận hành, bảo trì, kiểm tra, đánh giá, xử lý sự cố, nâng cấp, thay thế hoặc dừng khai thác.

3. Đối với phần mềm thương mại, dịch vụ công nghệ số, nền tảng dùng chung hoặc trường hợp không bàn giao mã nguồn, hồ sơ phải xác nhận quyền quản lý, khai thác, kết xuất, sao lưu, phục hồi, chuyển giao, trả về và xoá dữ liệu khi chấm dứt sử dụng.

4. Hệ thống thông tin chỉ được công bố đưa vào vận hành chính thức sau khi hoàn thành bàn giao và xác định rõ đơn vị vận hành, đầu mối hỗ trợ, đầu mối nghiệp vụ, đầu mối dữ liệu, đầu mối an ninh mạng và phương án xử lý sự cố.

Chương VI
QUẢN LÝ, VẬN HÀNH, BẢO TRÌ VÀ KẾT THÚC VÒNG ĐỜI

Điều 26. Quản lý, vận hành, bảo trì và giám sát chất lượng dịch vụ

1. Hệ thống thông tin sau khi đưa vào vận hành chính thức phải được quản lý, vận hành theo quy trình vận hành, quy chế sử dụng, phương án an ninh mạng, phương án sao lưu, phục hồi, phương án xử lý sự cố và hồ sơ bàn giao đã được phê duyệt hoặc xác nhận.

2. Nội dung vận hành thường xuyên gồm quản lý tài khoản, phân quyền, cấu hình, dung lượng, hiệu năng, nhật ký, sao lưu, phục hồi, hỗ trợ người dùng, xử lý lỗi, xử lý sự cố, theo dõi chất lượng dịch vụ, cập nhật tài liệu và báo cáo tình trạng vận hành.

3. Việc quản lý tài khoản, phân quyền phải thực hiện theo nguyên tắc định danh rõ người dùng, phân quyền tối thiểu cần thiết, tách biệt tài khoản quản trị, tài khoản người dùng, tài khoản tích hợp; cấp, thay đổi, thu hồi quyền kịp thời khi người dùng thay đổi nhiệm vụ hoặc không còn nhu cầu sử dụng.

4. Nhật ký vận hành, nhật ký truy cập, nhật ký thay đổi, nhật ký sự cố phải được thu thập, lưu trữ, bảo vệ, phân quyền khai thác và bảo đảm khả năng truy vết theo quy định.

5. Bảo hành hệ thống thông tin là nghĩa vụ của nhà thầu, đơn vị cung cấp sản phẩm, dịch vụ trong thời hạn xác định theo hợp đồng, hồ sơ được phê duyệt và quy định của pháp luật chuyên ngành; thời hạn bảo hành được xác định theo nhóm dự án, nhiệm vụ, sản phẩm hoặc thoả thuận được phê duyệt nhưng không thấp hơn mức tối thiểu theo quy định hiện hành.

6. Bảo trì hệ thống thông tin là trách nhiệm quản lý, vận hành thường xuyên của cơ quan chủ quản hệ thống thông tin, đơn vị vận hành hoặc đơn vị được giao quản lý dịch vụ, được thực hiện sau khi hết thời hạn bảo hành hoặc trong quá trình vận hành theo kế hoạch bảo trì, yêu cầu an ninh mạng, an ninh dữ liệu, an toàn dữ liệu, chất lượng dịch vụ và mức độ quan trọng của hệ thống.

7. Đối với dịch vụ công nghệ số, phần mềm thương mại, nền tảng dùng chung, đơn vị vận hành hoặc đơn vị được giao quản lý dịch vụ phải theo dõi

chất lượng dịch vụ, thời gian sẵn sàng, thời gian phản hồi, kết quả xử lý yêu cầu, sự cố, bảo mật dữ liệu, cam kết của nhà cung cấp và mức độ hài lòng của người sử dụng.

Điều 27. Quản lý thay đổi, sao lưu, phục hồi và bảo đảm liên tục hoạt động

1. Mọi thay đổi về nghiệp vụ, chức năng, dữ liệu, cấu hình, tích hợp, hạ tầng, phân quyền, an ninh mạng, chính sách vận hành sau khi hệ thống thông tin đã triển khai phải được quản lý theo quy trình quản lý thay đổi.

2. Quy trình quản lý thay đổi gồm tiếp nhận yêu cầu, đánh giá tác động, phân loại thay đổi, phê duyệt, kiểm thử, triển khai, giám sát, xác nhận kết quả, cập nhật hồ sơ và thông báo cho các bên liên quan.

3. Trước khi thực hiện thay đổi trên môi trường vận hành chính thức phải có phương án sao lưu, phương án khôi phục phiên bản cũ và kế hoạch thông báo, hỗ trợ người dùng khi cần thiết; sau khi thay đổi hoàn thành phải cập nhật tài liệu kỹ thuật, tài liệu vận hành, cấu hình, danh mục dữ liệu, mô hình tích hợp, phân quyền, nhật ký và hồ sơ liên quan.

4. Phần mềm và dữ liệu của hệ thống thông tin phải có phương án sao lưu, phục hồi phù hợp với mức độ quan trọng, cấp độ của hệ thống thông tin, tính chất dữ liệu, yêu cầu vận hành liên tục và mức độ chấp nhận gián đoạn.

5. Bản sao lưu dữ liệu có chứa thông tin mật, dữ liệu cá nhân, dữ liệu cá nhân nhạy cảm, dữ liệu nội bộ nhạy cảm phải được bảo vệ, phân quyền, mã hoá hoặc áp dụng biện pháp an toàn phù hợp theo quy định. Khả năng phục hồi từ bản sao lưu phải được kiểm tra định kỳ theo kế hoạch, phù hợp với mức độ quan trọng, cấp độ, yêu cầu vận hành liên tục và mức độ rủi ro của hệ thống, đồng thời kiểm tra khi có thay đổi lớn hoặc theo yêu cầu của cấp có thẩm quyền; kết quả kiểm tra phải được lập hồ sơ.

6. Đối với hệ thống trọng yếu, hệ thống dùng chung quy mô lớn, hệ thống phục vụ lãnh đạo, chỉ đạo, điều hành, phải có phương án bảo đảm liên tục hoạt động, kịch bản xử lý gián đoạn, phân công trách nhiệm, cơ chế báo cáo và kế hoạch kiểm tra, thử nghiệm hoặc diễn tập xử lý sự cố phù hợp.

Điều 28. Xử lý sự cố

1. Sự cố liên quan đến hệ thống thông tin phải được tiếp nhận, phân loại, xử lý, khắc phục, báo cáo, rút kinh nghiệm và lưu hồ sơ theo quy trình xử lý sự cố.

2. Sự cố được phân loại theo mức độ ảnh hưởng đến hoạt động nghiệp vụ, dữ liệu, an ninh mạng, an ninh dữ liệu, an toàn dữ liệu, thông tin mật, người dùng, phạm vi kết nối, chất lượng dịch vụ và khả năng vận hành liên tục.

3. Khi xảy ra sự cố, đơn vị vận hành chủ trì hoặc phối hợp thực hiện biện pháp cô lập, khôi phục, chuyển phương án dự phòng, thông báo đầu mối liên quan, bảo vệ nhật ký, bảo vệ hiện trường kỹ thuật, xác định nguyên nhân, khắc phục và báo cáo theo quy định.

4. Đối với sự cố có nguy cơ lộ, mất, sai lệch thông tin mật, dữ liệu cá nhân, dữ liệu hạn chế truy cập hoặc sự cố có dấu hiệu tấn công mạng, phải thực hiện ngay biện pháp kiểm soát khẩn cấp, bảo vệ chứng cứ, báo cáo cấp có thẩm quyền và phối hợp với cơ quan chuyên trách theo quy định.

5. Đối với sự cố an ninh mạng nghiêm trọng, sự cố ảnh hưởng lớn đến hoạt động của cơ quan Đảng, dữ liệu, thông tin mật hoặc có dấu hiệu xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, đơn vị vận hành phải thực hiện báo cáo ban đầu ngay sau khi phát hiện và trong thời hạn theo quy định của pháp luật, quy chế hoặc phương án ứng cứu sự cố được cấp có thẩm quyền phê duyệt; đồng thời thực hiện báo cáo bổ sung, báo cáo kết thúc sự cố theo quy định.

6. Sau khi xử lý sự cố, phải lập báo cáo nêu rõ thời gian, phạm vi, nguyên nhân, ảnh hưởng, dữ liệu liên quan, biện pháp đã thực hiện, kết quả khắc phục, kiến nghị phòng ngừa và trách nhiệm của các bên liên quan.

7. Trường hợp sự cố xảy ra do nguyên nhân khách quan, bất khả kháng hoặc vượt quá khả năng kiểm soát hợp lý, mặc dù cơ quan, đơn vị, cá nhân có trách nhiệm đã thực hiện đúng quy trình và biện pháp cần thiết trong phạm vi được giao, thì ưu tiên áp dụng ngay biện pháp khẩn cấp để cô lập, ngăn chặn, khắc phục, phục hồi hệ thống, bảo vệ dữ liệu, bảo toàn nhật ký, chứng cứ kỹ thuật và duy trì hoạt động nghiệp vụ.

Điều 29. Đánh giá hiệu quả, dừng khai thác, chuyển giao, thay thế, thanh lý hoặc huỷ bỏ hệ thống

1. Hệ thống thông tin phải được đánh giá định kỳ hằng năm hoặc đột xuất về hiệu quả khai thác, mức độ đáp ứng yêu cầu nghiệp vụ, mức độ tuân thủ Khung và Kiến trúc số có liên quan, mức độ sử dụng và tái sử dụng thành phần dùng chung, chất lượng dữ liệu, an ninh mạng, chất lượng vận hành, chất lượng dịch vụ, chi phí vòng đời và nhu cầu tiếp tục vận hành, hợp nhất, nâng cấp, thay thế hoặc dừng khai thác.

2. Chủ quản dữ liệu đánh giá chất lượng dữ liệu; đơn vị chủ trì sử dụng đánh giá hiệu quả nghiệp vụ; đơn vị vận hành đánh giá tình trạng kỹ thuật, vận hành, sự cố; đơn vị chuyên trách chuyển đổi số, an ninh mạng, cơ yếu tham gia đánh giá theo phạm vi trách nhiệm.

3. Kết quả đánh giá là căn cứ để quyết định tiếp tục vận hành, tối ưu, bảo trì, nâng cấp, mở rộng, hợp nhất, thay thế, dừng khai thác, thanh lý, huỷ bỏ hoặc điều chỉnh phương án quản lý, vận hành, phương án bảo vệ an ninh mạng và phương án xử lý dữ liệu; đồng thời cập nhật trạng thái vòng đời và tài liệu Kiến trúc số có liên quan khi quyết định làm thay đổi kiến trúc.

4. Việc dừng khai thác, chuyển giao, thay thế, thanh lý hoặc huỷ bỏ hệ thống thông tin phải có phương án được phê duyệt, trong đó xác định lý do, phạm vi, thời điểm, người dùng bị ảnh hưởng, dữ liệu, tài khoản, cấu hình, bản sao lưu, nhật ký, tài sản kỹ thuật, hợp đồng, dịch vụ liên quan, rủi ro và biện pháp xử lý.

5. Phương án xử lý dữ liệu phải làm rõ dữ liệu cần chuyển đổi, dữ liệu cần lưu trữ, dữ liệu cần tiêu huỷ, thời hạn lưu trữ, quyền truy cập, trách nhiệm chủ quản dữ liệu, trách nhiệm đơn vị quản trị dữ liệu, biện pháp bảo vệ thông tin mật, dữ liệu cá nhân, dữ liệu hạn chế truy cập và biện pháp kết thúc khai thác an toàn đối với tài khoản, quyền truy cập, bản sao lưu, nhật ký, khoá, cấu hình và tài sản kỹ thuật có liên quan.

6. Đối với hệ thống thuê dịch vụ, thuê phát triển, thuê vận hành hoặc sử dụng nền tảng của nhà cung cấp, trước khi chấm dứt hợp đồng hoặc chuyển sang nhà cung cấp khác phải thực hiện quy trình trả về dữ liệu, bàn giao cấu hình, tài khoản, nhật ký, tài liệu, bản sao lưu cuối cùng, thu hồi quyền truy cập và xác nhận xoá dữ liệu tại nhà cung cấp theo hợp đồng hoặc thoả thuận được phê duyệt.

Điều 30. Quản lý Cổng ứng dụng và ứng dụng thành phần trên Cổng

1. Việc tích hợp phần mềm, ứng dụng, dịch vụ số lên Cổng ứng dụng nội bộ hoặc cổng/nền tảng dùng chung trong các cơ quan Đảng phải thực hiện theo quy định, hướng dẫn về Cổng ứng dụng, định danh, xác thực, phân quyền, kết nối, chia sẻ dữ liệu và bảo vệ an ninh mạng.

2. Hồ sơ đề nghị tích hợp ứng dụng lên Cổng ứng dụng phải làm rõ tên ứng dụng, chủ quản hệ thống, đơn vị chủ trì sử dụng, đơn vị vận hành, chủ quản dữ liệu, phạm vi người dùng, phương thức xác thực, phân quyền, dữ liệu xử lý, kết nối, nhật ký, hỗ trợ kỹ thuật và phương án xử lý sự cố.

3. Cơ quan, đơn vị quản lý Cổng ứng dụng phối hợp với chủ quản hệ thống, đơn vị vận hành, đơn vị chuyên trách về an ninh mạng để kiểm soát việc tích hợp, vận hành, giám sát, xử lý sự cố, tạm dừng hoặc gỡ bỏ ứng dụng thành phần khi cần thiết.

Chương VII
TỔ CHỨC THỰC HIỆN

Điều 31. Rà soát hệ thống thông tin đã vận hành

1. Các hệ thống thông tin đã có quyết định đưa vào vận hành chính thức trước ngày Quyết định này có hiệu lực tiếp tục được khai thác, nhưng cơ quan chủ quản hệ thống thông tin có trách nhiệm rà soát, xác định phạm vi hệ thống, phân loại hệ thống, phân loại thông tin, phân loại dữ liệu, cập nhật hồ sơ, đánh giá rủi ro an ninh mạng, xác định hoặc xác định lại cấp độ của hệ thống thông tin, hoàn thiện hồ sơ xác định cấp độ, phương án bảo vệ an ninh mạng theo cấp độ, phương án bảo đảm an ninh dữ liệu, an toàn dữ liệu, sao lưu, phục hồi, quản lý thay đổi, quy chế vận hành và hồ sơ vận hành theo Quy định này và quy định về bảo vệ an ninh mạng đối với hệ thống thông tin theo cấp độ.

2. Nội dung rà soát gồm phạm vi sử dụng, chức năng nghiệp vụ, đối tượng sử dụng, đối tượng vận hành, chủ quản hệ thống, đơn vị chủ trì sử dụng, đơn vị vận hành, chủ quản dữ liệu, đơn vị quản trị dữ liệu, nguồn dữ liệu có thẩm quyền, cấp độ của hệ thống thông tin, hồ sơ xác định cấp độ, phương án bảo vệ an ninh mạng theo cấp độ, đánh giá rủi ro an ninh mạng, hồ sơ kỹ thuật, hồ sơ dữ liệu, hồ sơ vận hành, hồ sơ bàn giao, hợp đồng dịch vụ, quyền dữ liệu, phương án sao lưu, phục hồi, sự cố, kết nối, chia sẻ dữ liệu; khả năng sử dụng lõi số dùng chung, tình trạng trùng lặp và mức độ phù hợp với Khung Kiến trúc số trong các cơ quan Đảng và các tài liệu Kiến trúc số có liên quan.

3. Đối với hệ thống có xử lý thông tin mật, dữ liệu cá nhân, dữ liệu hạn chế truy cập hoặc hệ thống trọng yếu, cơ quan chủ quản hệ thống thông tin phải ưu tiên rà soát yêu cầu bảo vệ bí mật nhà nước, an ninh mạng, phân quyền, nhật ký, sao lưu, phục hồi, xử lý sự cố và điều kiện tham gia của nhà thầu, nhà cung cấp dịch vụ. Đối với hệ thống thông tin đã được xác định cấp độ theo quy định trước đây, việc rà soát, bổ sung, hoàn thiện điều kiện, tiêu chuẩn, biện pháp bảo vệ an ninh mạng thực hiện theo điều khoản chuyển tiếp của Nghị định số 331/2026/NĐ-CP và các quy định có liên quan.

4. Đối với hệ thống thuê dịch vụ, phần mềm thương mại, nền tảng dùng chung đang sử dụng, phải rà soát quyền quản lý, khai thác, kết xuất, sao lưu, phục hồi, chuyển giao, trả về và xoá dữ liệu khi chấm dứt dịch vụ; trường hợp chưa được quy định rõ trong hợp đồng, thoả thuận hoặc hồ sơ sử dụng thì phải bổ sung, điều chỉnh theo thẩm quyền.

5. Kết quả rà soát là căn cứ để tiếp tục vận hành, bổ sung hồ sơ, chuẩn hoá, tích hợp, hợp nhất, nâng cấp, mở rộng, chuyển đổi, thay thế hoặc dừng khai thác hệ thống thông tin; trường hợp phát hiện trùng lặp với thành phần dùng chung, nguồn dữ liệu song song hoặc nội dung không còn phù hợp với kiến trúc mục tiêu phải xác định phương án và lộ trình khắc phục, hội tụ.

6. Trong thời hạn 06 tháng kể từ ngày Quyết định này có hiệu lực, cơ quan chủ quản hệ thống thông tin hoàn thành việc lập danh mục, phân loại, xác định chủ quản hệ thống, đơn vị vận hành, chủ quản dữ liệu, nhóm áp dụng và mức độ ưu tiên rà soát đối với các hệ thống đang vận hành. Việc bổ sung, hoàn thiện hồ sơ thực hiện theo lộ trình do cơ quan chủ quản phê duyệt, bảo đảm hoàn thành trong thời hạn 12 tháng; ưu tiên trước đối với hệ thống trọng yếu, hệ thống có xử lý thông tin mật, dữ liệu cá nhân nhạy cảm, dữ liệu nội bộ nhạy cảm, hệ thống dùng chung hoặc hệ thống có kết nối, chia sẻ dữ liệu rộng.

Điều 32. Trách nhiệm của Cục Chuyển đổi số - Cơ yếu

1. Là đơn vị đầu mối tham mưu, hướng dẫn, theo dõi, đôn đốc, kiểm tra việc thực hiện Quyết định này theo chức năng, nhiệm vụ được giao.

2. Tham mưu, hướng dẫn, đánh giá tuân thủ Kiến trúc số giải pháp, quản lý ngoại lệ kiến trúc, sử dụng lõi số dùng chung, nguồn dữ liệu có thẩm quyền, tiêu chuẩn kỹ thuật, tiêu chuẩn tích hợp, chia sẻ dữ liệu, định danh, xác thực, an ninh mạng, cơ yếu, bảo vệ bí mật nhà nước trong quá trình triển khai, vận hành hệ thống thông tin.

3. Cho ý kiến thẩm định hoặc hướng dẫn thẩm định đối với đầu bài, phương án xây dựng, triển khai, Kiến trúc số giải pháp, kết quả đánh giá tuân thủ và hồ sơ ngoại lệ kiến trúc khi thuộc phạm vi cần kiểm soát; đồng thời tham gia đối với hồ sơ xác định cấp độ, phương án bảo vệ an ninh mạng, phương án kết nối, chia sẻ dữ liệu, phương án vận hành, phương án xử lý sự cố theo phân cấp.

4. Chủ trì hoặc phối hợp với Bộ Công an, Bộ Quốc phòng, Ban Cơ yếu Chính phủ và cơ quan có thẩm quyền trong việc hướng dẫn, thẩm định, kiểm tra hoặc xử lý vấn đề về bảo vệ an ninh mạng đối với hệ thống thông tin từ cấp độ 3

trở lên, hệ thống thông tin quan trọng về an ninh quốc gia, hệ thống có xử lý thông tin mật, sử dụng cơ yếu, mật mã hoặc có yếu tố quốc phòng, an ninh theo quy định.

5. Chủ trì hoặc phối hợp xây dựng, cập nhật biểu mẫu khuyến nghị, hướng dẫn kỹ thuật, tiêu chí phân loại, tiêu chí chất lượng dịch vụ, tiêu chí đánh giá tuân thủ, mẫu hồ sơ ngoại lệ kiến trúc và yêu cầu hồ sơ hoàn thành để tổ chức thực hiện thống nhất. Việc hướng dẫn, cập nhật không được làm thay đổi phạm vi điều chỉnh, đối tượng áp dụng, nguyên tắc, trách nhiệm hoặc làm phát sinh thủ tục bắt buộc ngoài Quy định này và quy định của cấp có thẩm quyền. Tổng hợp khó khăn, vướng mắc, kiến nghị sửa đổi, bổ sung Quy định, báo cáo lãnh đạo Văn phòng Trung ương Đảng xem xét, quyết định theo thẩm quyền.

Điều 33. Trách nhiệm của các cơ quan, đơn vị, cá nhân

1. Các cơ quan, đơn vị thuộc phạm vi áp dụng có trách nhiệm tổ chức thực hiện Quyết định này; rà soát, phân loại hệ thống thông tin thuộc phạm vi quản lý; xác định rõ cơ quan chủ quản hệ thống, đơn vị chủ trì sử dụng, đơn vị vận hành, chủ quản dữ liệu, đơn vị quản trị dữ liệu và các đầu mối liên quan.

2. Cơ quan, đơn vị có trách nhiệm bố trí hoặc đề xuất cấp có thẩm quyền bố trí nhân lực, kinh phí thường xuyên, nguồn lực và điều kiện kỹ thuật cần thiết cho vận hành, bảo trì, sao lưu, kiểm thử, diễn tập xử lý sự cố, bảo vệ an ninh mạng, bảo vệ bí mật nhà nước, bảo vệ dữ liệu, quản lý hồ sơ, tài liệu và thực hiện Quyết định này.

3. Các đơn vị chuyên trách chuyển đổi số, an ninh mạng, cơ yếu, dữ liệu, tài chính, đầu tư, mua sắm, pháp chế, văn thư - lưu trữ và các đơn vị liên quan có trách nhiệm phối hợp thực hiện theo chức năng, nhiệm vụ được giao.

4. Việc kiểm tra, giám sát định kỳ hằng năm hoặc đột xuất thực hiện Quyết định này được thực hiện theo yêu cầu quản lý, yêu cầu bảo vệ an ninh mạng, bảo vệ bí mật nhà nước, quản lý dữ liệu, vận hành và sử dụng hiệu quả hệ thống.

5. Trường hợp phát hiện vi phạm có nguy cơ ảnh hưởng đến an ninh mạng, bảo vệ bí mật nhà nước, dữ liệu cá nhân, dữ liệu hạn chế truy cập, vận hành hệ thống hoặc quyền quản lý dữ liệu của cơ quan Đảng, cơ quan có thẩm quyền có trách nhiệm yêu cầu tạm dừng, cô lập, khắc phục, thu hồi quyền truy cập, bổ sung hồ sơ, thay đổi phương án vận hành hoặc áp dụng biện pháp xử lý cần thiết. Tổ chức, cá nhân vi phạm thì tuỳ tính chất, mức độ bị xem xét xử lý theo quy định của Đảng, pháp luật của Nhà nước và quy chế nội bộ có liên quan.

6. Việc xem xét trách nhiệm đối với sự cố an ninh mạng, sự cố dữ liệu, sự cố vận hành hệ thống thông tin phải căn cứ nguyên nhân, phạm vi trách nhiệm được giao, mức độ tuân thủ quy trình, biện pháp đã thực hiện và kết quả khắc phục; thực hiện theo quy định của Đảng, pháp luật của Nhà nước và quy chế nội bộ có liên quan.

Điều 34. Quy định chuyển tiếp

1. Hệ thống thông tin bắt đầu thực hiện sau ngày Quyết định này có hiệu lực phải áp dụng Quyết định này theo nhóm hệ thống, hình thức triển khai, cấp độ của hệ thống thông tin, mức độ mật, phạm vi dữ liệu và trách nhiệm của các chủ thể liên quan.

2. Đối với nhiệm vụ, dự án, hoạt động mua sắm, thuê dịch vụ, xây dựng, nâng cấp, mở rộng hệ thống thông tin đã được phê duyệt hoặc đang triển khai chính thức trước ngày Quyết định này có hiệu lực, tiếp tục thực hiện theo hồ sơ đã được cấp có thẩm quyền phê duyệt; đồng thời rà soát, bổ sung yêu cầu của Quyết định này đối với các bước chưa thực hiện hoặc chưa hoàn thành, nhất là về sự phù hợp với Khung và Kiến trúc số có liên quan, khả năng dùng chung, nguồn dữ liệu có thẩm quyền, Kiến trúc số giải pháp khi thuộc trường hợp phải xây dựng, dữ liệu, an ninh mạng, bảo vệ bí mật nhà nước, bảo vệ dữ liệu cá nhân, kiểm thử, nghiệm thu, bàn giao, vận hành và hồ sơ hoàn thành.

3. Trường hợp việc bổ sung yêu cầu theo Quyết định này làm thay đổi mục tiêu, phạm vi, kiến trúc, công nghệ, dữ liệu, cấp độ của hệ thống thông tin, tiến độ, chi phí hoặc thẩm quyền phê duyệt, chủ đầu tư hoặc đơn vị được giao quản lý nhiệm vụ, dự án phải báo cáo cấp có thẩm quyền xem xét, quyết định trước khi thực hiện.

Điều 35. Tổ chức thực hiện

1. Các cơ quan, đơn vị thuộc phạm vi áp dụng tổ chức thực hiện Quy định này theo trách nhiệm quy định tại Điều 32 và Điều 33 của Quy định này.

2. Trong quá trình thực hiện, nếu phát sinh khó khăn, vướng mắc hoặc yêu cầu sửa đổi, bổ sung, các cơ quan, đơn vị phản ánh về Cục Chuyển đổi số - Cơ yếu để tổng hợp, báo cáo Chánh Văn phòng Trung ương Đảng xem xét, quyết định hoặc báo cáo cấp có thẩm quyền đối với nội dung vượt thẩm quyền.

PHỤ LỤC I
DANH MỤC PHÂN LOẠI HỆ THỐNG THÔNG TIN VÀ NHÓM ÁP DỤNG

(Kèm theo Quy định về xây dựng, triển khai, nghiệm thu, quản lý và vận hành hệ thống thông tin trong các cơ quan Đảng)

STT	Tiêu chí phân loại	Dấu hiệu nhận diện	Nhóm áp dụng đề xuất	Ghi chú
1	Tính chất thông tin xử lý	Có tạo lập, xử lý, lưu trữ, truyền đưa, hiển thị, khai thác, tích hợp hoặc sao lưu thông tin thuộc danh mục bí mật nhà nước.	Đầy đủ	Không áp dụng rút gọn đối với yêu cầu bảo vệ bí mật nhà nước, cơ yếu, an ninh mạng, nhật ký, sao lưu, phục hồi và xử lý sự cố.
2	Dữ liệu nhạy cảm, hạn chế truy cập	Có xử lý dữ liệu cá nhân nhạy cảm, dữ liệu nội bộ nhạy cảm, dữ liệu hạn chế truy cập hoặc dữ liệu có ảnh hưởng lớn đến tổ chức, cán bộ, tài chính, tài sản, vận hành.	Đầy đủ hoặc đặc thù	Việc phân nhóm căn cứ phạm vi người dùng, kết nối, chia sẻ dữ liệu, mức độ tác động và hình thức triển khai.
3	Mức độ quan trọng của hệ thống	Hệ thống phục vụ lãnh đạo, chỉ đạo, điều hành; hệ thống dùng chung; hệ thống nếu gián đoạn, mất dữ liệu, sai lệch dữ liệu hoặc bị tấn công sẽ ảnh hưởng lớn đến hoạt động của cơ quan Đảng.	Đầy đủ	Cần xác định yêu cầu vận hành liên tục, sao lưu, phục hồi, giám sát và xử lý sự cố.
4	Phạm vi dùng chung, kết nối, chia sẻ dữ liệu	Hệ thống dùng chung trong nhiều đơn vị, nhiều cấp; có kết nối, tích hợp, chia sẻ dữ liệu với hệ thống khác hoặc cơ quan, tổ chức khác trong hệ thống chính trị.	Đầy đủ	Cần hồ sơ kết nối, tích hợp, chia sẻ dữ liệu, phân quyền, nhật ký, truy vết và trách nhiệm phối hợp vận hành.
5	Quy mô nhỏ, nội bộ, ít rủi ro	Hệ thống nội bộ, ít người dùng, ít kết nối, không xử lý thông tin mật, không xử lý dữ liệu nhạy cảm, không ảnh hưởng lớn đến nghiệp vụ nếu gián đoạn.	Rút gọn	Có thể rút gọn hồ sơ, mô hình và kiểm thử, nhưng vẫn phải bảo đảm phân quyền, sao lưu, phục hồi, yêu cầu cơ bản về an ninh mạng và đầu mối vận hành.
6	Hình thức triển khai đặc thù	Phần mềm thương mại, dịch vụ công nghệ số, nền tảng dùng chung, dịch vụ điện toán đám mây, thuê dịch vụ, tiếp nhận chuyển giao, tài trợ, sử dụng thử hoặc phối hợp khai thác.	Đặc thù	Trọng tâm là quyền dữ liệu, quyền quản trị, trách nhiệm nhà cung cấp, chất lượng dịch vụ, bảo mật, kết xuất, sao lưu, phục hồi, chuyển giao, trả về và xoá dữ liệu.
7	Thay đổi, nâng cấp, chuyển đổi hoặc kết thúc vòng đời	Thay đổi chức năng, dữ liệu, tích hợp, hạ tầng, phân quyền, cấp độ của hệ thống thông tin; nâng cấp, thay thế, dừng khai thác, chuyển giao, thanh lý.	Theo phạm vi tác động	Căn cứ mức độ thay đổi để áp dụng đầy đủ, rút gọn hoặc đặc thù; phải có đánh giá tác động và hồ sơ xử lý tương ứng.

2. Nhóm áp dụng

Nhóm áp dụng	Đối tượng áp dụng chủ yếu	Yêu cầu tối thiểu	Lưu ý
Nhóm áp dụng đầy đủ	Hệ thống trọng yếu, quan trọng, dùng chung; hệ thống có xử lý thông tin mật, dữ liệu nhạy cảm; hệ thống có kết nối, chia sẻ dữ liệu rộng hoặc yêu cầu vận hành liên tục.	Đầy đủ hồ sơ theo vòng đời; mô hình kiến trúc; hồ sơ dữ liệu; hồ sơ an ninh mạng; kiểm thử, nghiệm thu, bàn giao, vận hành, sao lưu, phục hồi, xử lý sự cố và giám sát.	Áp dụng mức kiểm soát cao hơn khi hệ thống đồng thời thuộc nhiều tiêu chí rủi ro.
Nhóm áp dụng rút gọn	Hệ thống nội bộ quy mô nhỏ, ít người dùng, ít kết nối, cấp độ 1, cấp độ 2, không xử lý thông tin mật, không xử lý dữ liệu nhạy cảm.	Hồ sơ tối thiểu; đầu bài hoặc tài liệu tương đương; kiểm thử chức năng, dữ liệu, phân quyền, sao lưu, phục hồi; biên bản nghiệm thu, bàn giao; đầu mối vận hành.	Không rút gọn yêu cầu tuân thủ pháp luật, bảo vệ dữ liệu cá nhân, an ninh mạng và trách nhiệm vận hành.
Nhóm áp dụng đặc thù	Phần mềm thương mại, dịch vụ công nghệ số, nền tảng dùng chung, dịch vụ điện toán đám mây, thuê dịch vụ, tiếp nhận chuyển giao, tài trợ, sử dụng thử, phối hợp khai thác.	Hồ sơ tập trung vào điều kiện sử dụng, hợp đồng/thoả thuận, quyền dữ liệu, quyền quản trị, trách nhiệm nhà cung cấp, an ninh mạng, chất lượng dịch vụ, sao lưu, phục hồi, chuyển giao, trả về và xoá dữ liệu.	Không bắt buộc hồ sơ thiết kế, mã nguồn nếu không phù hợp hình thức triển khai; phải có căn cứ thay thế để nghiệm thu và vận hành.

PHỤ LỤC II
DANH MỤC KIỂM TRA TRƯỚC NGHIỆM THU, BÀN GIAO VÀ VẬN HÀNH CHÍNH THỨC

(Kèm theo Quy định số về xây dựng, triển khai, nghiệm thu, quản lý và vận hành hệ thống thông tin trong các cơ quan Đảng)

Mục đích, yêu cầu: Phụ lục này là bảng kiểm ở mức danh mục, sử dụng trước khi nghiệm thu, bàn giao và đưa hệ thống thông tin vào vận hành chính thức.

Kết luận đạt/chưa đạt do chủ đầu tư hoặc đơn vị được giao quản lý nhiệm vụ, dự án tổng hợp trên cơ sở xác nhận của các đơn vị có trách nhiệm.

STT	Nội dung kiểm tra	Áp dụng	Tài liệu hoặc bằng chứng	Đơn vị xác nhận	Kết luận
1	Mục tiêu, phạm vi, đối tượng sử dụng, yêu cầu nghiệp vụ, hình thức thiết kế một bước hoặc hai bước và tiêu chí nghiệm thu đã được đối chiếu với đầu bài, phương án được phê duyệt.	Mọi hệ thống	Đầu bài, phương án, hồ sơ thiết kế, biên bản kiểm thử, biên bản nghiệm thu sử dụng	Đơn vị chủ trì sử dụng	Đạt/Chưa đạt
2	Chức năng chính, biểu mẫu, báo cáo, thống kê, tra cứu, phê duyệt và phân quyền nghiệp vụ đáp ứng yêu cầu sử dụng.	Mọi hệ thống	Kịch bản kiểm thử, kết quả kiểm thử, xác nhận người dùng	Đơn vị chủ trì sử dụng	Đạt/Chưa đạt
3	Dữ liệu đầu vào, đầu ra, danh mục dữ liệu, dữ liệu dùng chung, dữ liệu tham chiếu và dữ liệu kế thừa đã được xác nhận.	Hệ thống có xử lý dữ liệu nghiệp vụ	Danh mục dữ liệu, báo cáo đối soát, xác nhận chủ quản dữ liệu	Chủ quản dữ liệu	Đạt/Chưa đạt
4	Dữ liệu kế thừa đã được chuyển đổi, làm sạch, chuẩn hoá, đối soát trước khi nghiệm thu hoặc đưa vào vận hành chính thức.	Hệ thống nâng cấp, thay thế, tích hợp, chuyển đổi dữ liệu	Báo cáo chuyển đổi dữ liệu, biên bản đối soát, biên bản xác nhận dữ liệu	Chủ quản dữ liệu, đơn vị quản trị dữ liệu	Đạt/Chưa đạt
5	Kết nối, tích hợp, chia sẻ dữ liệu đúng mục đích, đúng thẩm quyền, đúng phạm vi và có khả năng truy vết.	Hệ thống có tích hợp, chia sẻ dữ liệu	Hồ sơ kết nối, đặc tả API, nhật ký thử nghiệm, biên bản kiểm thử tích hợp	Đơn vị chuyên trách chuyển đổi số, đơn vị vận hành	Đạt/Chưa đạt
6	Tài khoản, phân quyền, xác thực, tài khoản quản trị, tài khoản người dùng và tài khoản tích hợp được cấu hình đúng nguyên tắc phân quyền tối thiểu cần thiết.	Mọi hệ thống	Danh sách tài khoản, ma trận phân quyền, biên bản kiểm tra cấu hình	Đơn vị vận hành, đơn vị chuyên trách về an ninh mạng	Đạt/Chưa đạt

STT	Nội dung kiểm tra	Áp dụng	Tài liệu hoặc bằng chứng	Đơn vị xác nhận	Kết luận
7	Nhật ký truy cập, nhật ký vận hành, nhật ký thay đổi, nhật ký tích hợp và nhật ký sự cố được bật, lưu trữ, bảo vệ và truy vết được.	Mọi hệ thống	Biên bản kiểm tra nhật ký, cấu hình lưu nhật ký, mẫu nhật ký	Đơn vị vận hành	Đạt/Chưa đạt
8	Phương án sao lưu, phục hồi, quay lui và xử lý sự cố được lập, kiểm tra và xác nhận phù hợp với mức độ quan trọng của hệ thống.	Mọi hệ thống; bắt buộc đối với hệ thống quan trọng, trọng yếu, dùng chung	Phương án sao lưu, phục hồi, kết quả kiểm tra phục hồi, kịch bản xử lý sự cố	Đơn vị vận hành, đơn vị chuyên trách về an ninh mạng	Đạt/Chưa đạt
9	Hồ sơ xác định cấp độ của hệ thống thông tin, phương án bảo vệ an ninh mạng theo cấp độ, kết quả thẩm định/phê duyệt và kết quả kiểm tra, đánh giá, kiểm thử an ninh mạng đáp ứng yêu cầu trước khi nghiệm thu, bàn giao, vận hành chính thức.	Từ lập phương án, trước phê duyệt thiết kế hoặc phương án kỹ thuật; hoàn thành trước vận hành chính thức	Hồ sơ xác định cấp độ; phương án bảo vệ an ninh mạng theo cấp độ; văn bản thẩm định/phê duyệt; báo cáo kiểm thử an ninh mạng; biên bản khắc phục lỗ hổng.	Thực hiện theo quy định về bảo vệ an ninh mạng đối với hệ thống thông tin theo cấp độ; trường hợp cấp độ 4, cấp độ 5 hoặc hệ thống thuộc diện phải xin ý kiến, thẩm định của cơ quan chuyên trách thì thực hiện theo thẩm quyền quy định.	Đạt/Chưa đạt
10	Điều kiện bảo vệ bí mật nhà nước, cơ yếu, dữ liệu cá nhân nhạy cảm, dữ liệu nội bộ nhạy cảm, dữ liệu hạn chế truy cập được kiểm tra khi có phát sinh.	Hệ thống có thông tin mật, dữ liệu nhạy cảm hoặc hạn chế truy cập	Hồ sơ bảo mật, phân vùng, kiểm soát truy cập, danh sách nhân sự, biên bản kiểm tra	Đơn vị chuyên trách về an ninh mạng, cơ yếu, chủ quản dữ liệu	Đạt/Chưa đạt
11	Hiệu năng, khả năng sẵn sàng, dung lượng, khả năng mở rộng, chất lượng dịch vụ, kiểm thử độc lập khi có yêu cầu và vận hành thử tại đơn vị thụ hưởng được kiểm tra trong phạm vi cần thiết.	Hệ thống quan trọng, dùng chung, nhiều người dùng hoặc thuê dịch vụ	Báo cáo kiểm thử hiệu năng, báo cáo kiểm thử độc lập, báo cáo vận hành thử tại đơn vị thụ hưởng, báo cáo chất lượng dịch vụ	Chủ đầu tư, đơn vị vận hành	Đạt/Chưa đạt

STT	Nội dung kiểm tra	Áp dụng	Tài liệu hoặc bằng chứng	Đơn vị xác nhận	Kết luận
12	Đơn vị vận hành đã tiếp nhận tài liệu vận hành, cấu hình, quyền quản trị, đầu mối hỗ trợ, tài sản kỹ thuật và hồ sơ bàn giao.	Mọi hệ thống	Biên bản bàn giao, danh mục hồ sơ hoàn thành, danh mục tài sản kỹ thuật	Đơn vị vận hành	Đạt/Chưa đạt
13	Đối với phần mềm thương mại, dịch vụ công nghệ số, nền tảng dùng chung, dịch vụ thuê, đã làm rõ quyền dữ liệu, quyền quản trị, kết xuất, sao lưu, phục hồi, trả về, xoá dữ liệu và cơ chế nghiệm thu định kỳ trong suốt thời hạn hợp đồng.	Nhóm áp dụng đặc thù	Hợp đồng, thoả thuận dịch vụ, tài liệu điều kiện sử dụng, biên bản xác nhận quyền dữ liệu, biên bản nghiệm thu định kỳ	Chủ đầu tư hoặc đơn vị được giao quản lý dịch vụ	Đạt/Chưa đạt
14	Đối với hệ thống có ứng dụng trí tuệ nhân tạo, đã xác định mục đích, phạm vi, loại dữ liệu, cơ chế kiểm soát đầu vào, đầu ra, giám sát của con người và biện pháp phòng ngừa lạm dụng, sai lệch, lộ lọt dữ liệu.	Hệ thống có ứng dụng trí tuệ nhân tạo	Nội dung ứng dụng AI trong phương án, biên bản kiểm tra, tài liệu giám sát	Đơn vị chủ trì sử dụng, chủ quản dữ liệu, đơn vị chuyên trách về an ninh mạng	Đạt/Chưa đạt
15	Đã hoàn thành đào tạo, hướng dẫn sử dụng, thông báo đầu mối hỗ trợ và phương thức tiếp nhận yêu cầu hỗ trợ người dùng.	Mọi hệ thống	Biên bản đào tạo, tài liệu hướng dẫn, danh sách đầu mối hỗ trợ	Đơn vị chủ trì sử dụng, đơn vị vận hành	Đạt/Chưa đạt
16	Hồ sơ hoàn thành đã được lập danh mục, lưu trữ tập trung, phân quyền truy cập và bảo vệ theo mức độ mật, mức độ nhạy cảm.	Mọi hệ thống	Danh mục hồ sơ hoàn thành, xác nhận lưu trữ, phân quyền truy cập	Chủ đầu tư hoặc đơn vị được giao quản lý nhiệm vụ, dự án	Đạt/Chưa đạt
17	Đã đánh giá tuân thủ Khung Kiến trúc số và Kiến trúc số có liên quan; đã rà soát lõi số dùng chung, nguồn dữ liệu có thẩm quyền, khả năng tái sử dụng và tránh trùng lặp; ngoại lệ kiến trúc (nếu có) đã được chấp thuận và còn hiệu lực.	Mọi hệ thống; Kiến trúc số giải pháp áp dụng theo Điều 18	Kết quả đánh giá tuân thủ; Kiến trúc số giải pháp; hồ sơ ngoại lệ kiến trúc; tài liệu rà soát dùng chung	Đơn vị chuyên trách chuyển đổi số, chủ quản dữ liệu và đơn vị liên quan	Đạt/Chưa đạt

Ghi chú: Trường hợp nội dung kiểm tra không áp dụng, đơn vị chủ trì tổng hợp ghi rõ "Không áp dụng" và nêu lý do trong hồ sơ nghiệm thu, bàn giao.

Ghi chú áp dụng bổ sung:

1. Không đưa hệ thống thông tin vào vận hành chính thức nếu các nội dung kiểm tra bắt buộc đối với hệ thống đó chưa đạt, đặc biệt là phân quyền, nhật ký, sao lưu, phục hồi, hồ sơ xác định cấp độ của hệ thống thông tin, kiểm thử an ninh mạng, điều kiện bảo vệ bí mật nhà nước, dữ liệu nhạy cảm và bàn giao vận hành.

2. Trường hợp phải vận hành tạm thời vì yêu cầu cấp bách, phải có phê duyệt của cấp có thẩm quyền, phương án kiểm soát rủi ro, thời hạn khắc phục và đầu mối chịu trách nhiệm.